Files are in Adobe format. Download the newest version from Adobe.

2009 Biometrics Conference

"Strategies for Implementing HSPD - 24"

Arlington, VA

27 - 28 January 2009

Agenda

Biometrics Conference Meeting Minutes, January 27-28, 2009

Tuesday 27 January 2008

Opening Remarks
- Ms. Martha Karlovic, Chair, NDIA Industrial Committee on Biometrics
- Mr. Thomas Giboney, NDIA Industrial Committee on Biometrics

Policy Panel Discussion
Panelists:
- Mr. Robert Mocny, Director, US-VISIT Program, Department of Homeland Security
- Mr. Al Miller, OSD - Policy, U.S. Department of Defense
- Mr. Thomas Bush, III, Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation
- Mr. Tony Edson, Senior Advisor, Consular Affairs, U.S. Department of State

Government Panel Discussion
Panelists:
- Ms. Kimberly DelGreco, Section Chief, Biometric Service Section, Federal Bureau of Investigation
- Mr. William Vickers, Special Advisor to the Director, Biometrics Task Force
- COL James Brown, USA, Chief, Force Protection & Mission Assurance, USNORTHCOM

Commercial Industry Panel Discussion
Panelists:
- Mr. Jason Slibeck, Chief Technology Officer, CLEAR
- Ms. Katherine Stokes, Associate General Counsel, Graduate Management Admission Council

Wednesday 28 January 2009

Keynote Speaker
Dr. David Boyd, Director, Command, Control, Interoperability, U.S. Department of Homeland Security

Technologies Panel Discussion

Panelists:

- Mr. Brad Wing, IT Specialist, National Institute of Standards and Technology
- Mr. Ken Martin, Past President, International Association for Identification
- Dr. Stephen Elliot, Associate Professor of Industrial Technology, Purdue University
- Dr. Arun Ross, Associate Professor, Lane Department of Computer Science and Electrical Engineering, West Virginia University

International Panel Discussion

Panelists:

- Mexico, Mr. Carlos Raul Anaya Moreno, Director General, National Register of Population and Personal Identification
- INTERPOL, Mr. Joseph Orrigo, Senior CI Advisor, Terrorism and Violent Crime Division

Interoperability Panel Discussion

Panelists:

- Mr. Paul Grant, Office of CIO, U.S. Department of Defense
- Mr. Paul Garrett, Special Assistant To The Chief Information Officer, Department of Justice
- Mr. Dirk Rankin, National Counterterrorism Center

NDIA
NATIONAL DEFENSE INDUSTRIAL ASSOCIATION
STRENGTH THROUGH INDUSTRY & TECHNOLOGY

PROMOTING NATIONAL SECURITY SINCE 1919

2009 BIOMETRICS CONFERENCE

"Strategies For Implementing HSPD - 24"

HIGHLIGHTS INCLUDE:

- Keynote Speakers
  - Senator Jeff Sessions, Alabama (Invited)
  - General Victor Renuart, Commander, NORTHCOM
  - Dr. David Boyd, Director, Command, Control, Interoperability, Department of Homeland Security
- Creating the framework for a biometric network to defeat a terrorist network.
- Sharing biometric and associated biographical and contextual information from Federal to State, local and tribal authorities.
- The Challenge: We need to find, understand and fix the gaps before our enemies do.
- Six focused Panel discussions with topical SMEs.

THE SHERATON NATIONAL HOTEL ▸ ARLINGTON, VA

EVENT #9860

JANUARY 27 - 28, 2009

WWW.NDIA.ORG/MEETINGS/9860

PROMOTIONAL PARTNERS:

AWARE

IBM

L-1 IDENTITY SOLUTIONS

LOCKHEED MARTIN

NetApp

Raytheon

SAIC
From Science to Solutions

NORTHROP GRUMMAN

PROMOTIONAL PARTNERSHIPS

Increase your company or organization exposure at this premier conference by becoming a Promotional Partner. A Promotional Partnership ($2,500) will add your logo to the website, company logo and a 350 word company description in the onsite brochure, podium recognition throughout the conference and signage at registration. For more information, please contact Britt Bommelje at 703-247-2587 or bbommelje@ndia.org.

2009 BIOMETRICS CONFERENCE

JANUARY 27, 2009 - JANUARY 28, 2009

SHERATON NATIONAL HOTEL ▸ ARLINGTON, VA

On 5 JUNE 2008, The President of the United States issued a national directive aimed at enhancing the security of our nation, its citizens and infrastructure, through the use and application of biometrics. The document is entitled, "Homeland Security Presidential Directive/HSPD – 24." The subject of the directive is, "Biometrics for Identification and Screening to Enhance National Security."

The Attorney General working with the Secretaries of State, Defense and Homeland Security, the Director of National Intelligence and the Director of the Office of Science and Technology is charged to develop an Action Plan for implementing HSPD-24 by June 2009. NDIA's Biometric Conference 2009 is designed to be an open forum for identifying and discussing practical approaches to the challenges of successfully implementing HSPD-24. The NDIA conference will examine a broad spectrum of issues ranging from:

- Policy development
- Existing and planned U.S. Government programs
- Examples of commercial application of biometrics to address mission critical business goals
- Enabling technologies
- Initiatives within the international community
- Challenges to achieving true interoperability and information sharing.

The conference's goal is to develop a mutual understanding and cardinal direction for possible solutions wherein jurisdiction gaps are closed, technologies are interoperable and policies are cohesive.

HSPD-24, "Biometrics for Identification and Screening to Enhance National Security," June 2008, creates the framework for a biometric network to defeat a terrorist network by "sharing of biometric and associated biographical and contextual information." It calls for "layered approach to identification and screening of individuals, as no single mechanism is sufficient" across multiple sovereign jurisdictions of Federal, States, local and tribal authorities. The Federal Government has responsibility for 115 airports, 14 seaports, 150 land ports, 220 consulates and two sea borders and the two land borders with numerous waterways. On that layer, add the 50 states and municipalities. HSPD-24 is challenged by multiple jurisdictions, different technologies and policies.

Please join us and share your skills and experience with other conference attendees and panelists so that we might truly identify some practical, achievable results with respect to the operational goals and objectives of HSPD-24 and make our world a safer place to live and work.

REGISTRATION INFORMATION

REGISTRATION

Register online by visiting the conference website at www.ndia.org/meetings/9860. Online registration will close at 5:00 pm EST on January 16, 2009. You may also fax the registration form found in this brochure to 703-522-1885 or mail to National Defense Industrial Association, Event #9860, 2111 Wilson Blvd., Suite 400, Arlington, VA 22201. Payment must be made at the time of registration. Registrations will not be taken over the phone. In order for your name to appear in the on-site attendee roster, you must register for the conference by January 16, 2009. After this date, you must register on-site.

CONFERENCE REGISTRTION FEES	EARLY (BEFORE 12/20/08)	REGULAR (12/20/08-1/16/09)	LATE (AFTER 1/16/09)
GOVERNMENT/ ACADEMIA/ ALLIED GOV.	$350	$385	$425
INDUSTRY NDIA MEMBER	$450	$495	$545
INDUSTRY NON-NDIA MEMBER	$525	$580	$640

CANCELLATION POLICY

Cancellations received before December 20, 2008 will receive a full refund. Cancellations received between December 20, 2008 and January 16, 2009 will receive a refund minus a $75 cancellation fee. No refunds will be given for cancellations received after January 16, 2009. Substitutions are welcome in lieu of cancellations. Cancellations and substitutions must be made in writing to Holley Slabaugh at hslabaugh@ndia.org.

COMPANIES THAT WILL BE DISPLAYING INCLUDE:

Iritech, Inc.

Booz Allen Hamilton

Hitachi America, LTD

SAIC

Aware, Inc.

L-1 Identity Solutions

SPECIAL NEEDS

NDIA supports the Americans with Disabilities Act of 1990. Attendees with special needs should call Holley Slabaugh at 703-247-2561 prior to January 16, 2009.

CONFERENCE ATTIRE

Appropriate dress for this symposium is business for civilians (coat and tie) and class A uniform or uniform of the day for military.

INQUIRES

For more information regarding the conference contact Holley Slabaugh, Meeting Planner, at 703-247-2561 or hslabaugh@ndia.org or Britt Bommelje, Director, Operations at 703-247-2587 or bbommelje@ndia.org.

PLANNING COMMITTEE

Martha Karlovic, SAIC
Richard Scott, IBM
Thomas Giboney, Biometrics Task Force
Timothy Hassell, L-3 Communications
James Jarboe, Lockheed Martin Corporation
Beth Lavach, Consortium of Forensic Science Organizations
Magruder Dent, AWARE, Inc.
Jeff Hathaway, L-1 Identity Solutions
Patrick Flynn, University of Notre Dame

LODGING

A block of rooms has been reserved at the Sheraton National Hotel. Both the government rate and industry rate is $179 US (Single and Double).

In order to ensure the discounted NDIA rate, please make reservations early and ask for the NDIA room block. Rooms will not be held after Friday, December 26, 2008 and may sell out before then. Rates are subject to increase after this date.

TUESDAY JANUARY 27 2009

7:00 am - 6:30 pm	**Registration Open**
7:00 am - 8:00 am	**Continental Networking Breakfast**
8:00 am - 8:10 am	**Administrative Remarks** MG Barry Bates, USA (Ret), Vice President, Operations, National Defense Industrial Association
8:10 am - 8:30 am	**Opening Remarks** Ms. Martha Karlovic, Chair, NDIA Industrial Committee on Biometrics Mr. Thomas Giboney, NDIA Industrial Committee on Biometrics
8:30 am - 9:00 am	**Keynote Speaker** The Honorable Jeff Sessions, Senator, Alabama (Invited)
9:00 am - 9:30 am	**Keynote Speaker** Gen Victor Renuart, Jr., USAF, Commander, North American Aerospace Defense Command and U.S. Northern Command, United States Department of Defense
9:30 am - 10:00 am	**Break**
10:00 am - 12:00 pm	**Policy Panel Discussion** ▸ Moderator: Mr. Jeffrey Hathaway, Vice President, L-1 Identity Solutions Panelists: ▸ *Mr. Robert Mocny, Director, US-VISIT Program, Department of Homeland Security* ▸ *Mr. Al Miller, OSD - Policy, U.S. Department of Defense* ▸ *Mr. Thomas Bush, III, Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation*
12:00 pm - 1:00 pm	**Lunch**
1:00 pm - 2:45 pm	**Government Panel Discussion** ▸ Moderator: Ms. Beth Lavach, ELS & Associate, Consortium of Forensic Science Organizations Panelists: ▸ *Ms. Kimberly DelGreco, Section Chief, Biometric Service Section, Federal Bureau of Investigation* ▸ *Mr. William Vickers, Special Advisor to the Director, Biometrics Task Force* ▸ *Ms. Angela Miller, Consular Affairs, U.S. Department of State* ▸ *COL James Brown, USA, Chief, Force Protection & Mission Assurance, USNORTHCOM* ▸ *Ms. Patricia Cogswell, Executive Director, Screening Coordination Office, U.S. Department of Homeland Security*
2:45 pm - 3:15 pm	**Break**

TUESDAY JANUARY 27 2009

3:15 pm - 4:45 pm

Commercial Industry Panel Discussion

- **Moderator: Ms. Martha Karlovic, Vice President, Security and Identity Management, SAIC**

Panelists:

- *Mr. Chris Swecker, Global Corporate Security Director, Bank of America*
- *Mr. Jason Slibeck, Chief Technology Officer, CLEAR*
- *Ms. Katherine Stokes, Associate General Counsel, Graduate Management Admission Council*

4:45 pm - 5:00 pm

Closing Remarks

Ms. Martha Karlovic, Chair, NDIA Industrial Committee on Biometrics

Mr. Thomas Giboney, NDIA Industrial Committee on Biometrics

5:00 pm - 6:30 pm

Networking Reception

WEDNESDAY JANUARY 28 2009

7:00 am - 3:45 pm

Registration Open

7:00 am - 8:15 am

Continental Networking Breakfast

8:15 am - 8:25 am

Administrative Remarks

MG Barry Bates, USA (Ret), Vice President, Operations, National Defense Industrial Association

8:25 am - 8:55 am

Keynote Speaker

Dr. David Boyd, Director, Command, Control, Interoperability, U.S. Department of Homeland Security

8:55 am - 9:40 am

Break

9:40 am - 11:40 am

Technologies Panel Discussion

- **Moderator: Mr. Timothy Hassell, Program Director, L-3 Communications**

Panelists:

- *Mr. Brad Wing, IT Specialist, National Institute of Standards and Technology*
- *Mr. Ken Martin, Past President, International Association for Identification*
- *Dr. Stephen Elliot, Associate Professor of Industrial Technology, Purdue University*
- *Dr. Marios Savvides, Director of Biometrics, CyLab*
- *Dr. Arun Ross, Associate Professor, Lane Department of Computer Science and Electrical Engineering, West Virginia University*

WEDNESDAY JANUARY 28 2009

11:40 am - 12:45 pm — **Lunch**

12:45 pm - 2:15 pm — **International Panel Discussion**

- **Moderator: Mr. Wiliam Vickers, Special Advisor to the Director, Biometrics Task Force**
  Panelists:
  - *United Kingdom*
  - *Mexico, Mr. Carlos Raul Anaya Moreno, Director General, National Register of Population and Personal Identification*
  - *INTERPOL, Mr. Joseph Orrigo, Senior CI Advisor, Terrorism and Violent Crime Division*

2:15 pm - 3:45 pm — **Interoperability Panel Discussion**

- **Moderator: Mr. Richard Scott, Director, IBM**
  Panelists:
  - *Mr. John Aslanes, Program Manager, NCTC Identities/Terrorist Identities Data Mart*
  - *Mr. Paul Grant, Office of CIO, U.S. Department of Defense*
  - *Mr. Thomas Lockwood, Senior Advisor, Screening Credential Office, U.S. Department of Homeland Security*
  - *Mr. Paul Garrett, Special Assistant To The Chief Information Officer, Department of Justice*

3:45 pm — **Closing Remarks**

Ms. Martha Karlovic, Chair, NDIA Industrial Committee on Biometrics

Mr. Thomas Giboney, NDIA Industrial Committee on Biometrics

EVENT #9860 ▸ NDIA REGISTRATION FORM

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION ▸ 2111 WILSON BOULEVARD, SUITE 400 ▸ ARLINGTON, VA 22201-3061
(703) 522-2561 ▸ (703) 522-1885 FAX ▸ WWW.NDIA.ORG/MEETINGS/9860

2009 BIOMETRICS CONFERENCE ▸ SHERATON NATIONAL HOTEL
ARLINGTON, VA ▸ JANUARY 27-28, 2009

3 WAYS TO SIGN UP:

1. **Online with a credit card at www.ndia.org**
2. **By fax with a credit card - Fax: (703) 522-1885**
3. **By mail with a check or credit card**

▷ Address Change Needed

NDIA Master ID/Membership # _____ Social Security # _____
(If known - hint: on mailing label above your name) *(Last 4 digits - optional)*

Prefix *(e.g. RADM, COL, Mr., Ms., Dr., etc.)* _____

Name: First _____ MI ____ Last _____

Military Affiliation _____ Nickname _____
(e.g. USMC, USA (Ret.) etc.) *(For meeting badges)*

Title _____

Organization _____

Street Address _____

Address *(Suite, PO Box, Mail Stop, Building, etc.)* _____

City _____ State _____ Zip _____ Country _____

Phone _____ Ext. _____ Fax _____

E-Mail _____

Signature* _____ Date _____

PREFERRED WAY TO RECEIVE INFORMATION

Conference Information	▷ Address above	▷ Alternate (Print address below)	▷ E-mail
Subscriptions	▷ Address above	▷ Alternate (Print address below)	

Alternate Street Address _____

Alternate Address *(Suite, PO Box, Mail Stop, Building, etc.)* _____

City _____ State _____ Zip _____ Country _____

* By your signature above, you consent to receive communications sent by or on behalf of NDIA, its Chapters, Divisions and affiliates (NTSA, AFEI, PSA, WID) through regular mail, e-mail, telephone or fax. NDIA, its Chapters, Divisions and affiliates do not sell data to vendors or other companies.

CONFERENCE REGISTRATION FEES

	Early *(Before 12/20/08)*	Regular *(12/20/08-1/16/09)*	Late *(After 1/16/09)*
Government/Academia[1]	$350	$385	$425
Industry NDIA Member and affiliates (AFEI, NTSA, PSA, WID)	$450	$495	$545
Industry non-NDIA member[2]	$525	$580	$640

Cancellations received before December 20, 2008 will receive a full refund. Cancellations received between December 20, 2008 and January 16, 2009 will receive a refund minus a $75 cancellation fee. No refunds will be given for cancellations received after January 16, 2009. Substitutions are welcome in lieu of cancellations. Cancellations and substitutions must be made in writing to hslabaugh@ndia.org.

[1] *Includes a free three-year NDIA membership and subscription to* National Defense *magazine for military and government employees.*

▷ No, do not sign me up for the free government membership.

[2] *Registration fees for non-NDIA (or affiliate) members include a one-year non-refundable NDIA membership —$15.00 will be applied for your 12 month subscription to* National Defense *magazine.*

PAYMENT OPTIONS

▷ **Check** (Payable to NDIA - Event #9860) ▷ **Government PO/Training Form #** _____

▷ **VISA** ▷ **MasterCard** ▷ **American Express** ▷ **Diners Club** ▷ **Cash**

If paying by credit card, you may return by fax to 703-522-1885.

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ Credit Card Number ☐☐/☐☐ Exp. Date

Signature _____ Date _____

BY COMPLETING THE FOLLOWING, YOU HELP US UNDERSTAND WHO IS ATTENDING OUR EVENTS.

PRIMARY OCCUPATIONAL CLASSIFICATION. Check ONE.

- ▷ Defense Business/Industry
- ▷ R&D/Laboratories
- ▷ Army
- ▷ Navy
- ▷ Air Force
- ▷ Marine Corps
- ▷ Coast Guard
- ▷ DOD/MOD Civilian
- ▷ Government Civilian (Non-DOD/MOD)
- ▷ Trade/Professional Assn.
- ▷ Educator/Academia
- ▷ Professional Services
- ▷ Non-Defense Business
- ▷ Other _____

CURRENT JOB/TITLE/POSITION. Check ONE.

- ▷ Senior Executive
- ▷ Executive
- ▷ Manager
- ▷ Engineer/Scientist
- ▷ Professor/Instructor/Librarian
- ▷ Ambassador/Attaché
- ▷ Legislator/Legislative Aide
- ▷ General/Admiral
- ▷ Colonel/Navy Captain
- ▷ Lieutenant Colonel/Commander/ Major/Lieutenant Commander
- ▷ Captain/Lieutenant/Ensign
- ▷ Enlisted Military
- ▷ Other _____

Year of birth _____
(optional)

QUESTIONS, CONTACT:

HOLLEY SLABAUGH, MEETING PLANNER

PHONE: 703-247-2561

E-MAIL: HSLABAUGH@NDIA.ORG

MAIL REGISTRATION TO:
NDIA - EVENT #9860
2111 WILSON BOULEVARD
SUITE 400
ARLINGTON, VA 22201

FAX TO: 703-522-1885

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION
STRENGTH THROUGH INDUSTRY & TECHNOLOGY

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION
2111 WILSON BOULEVARD, SUITE 400
ARLINGTON, VA 22201-3061
(703) 522-2561
(703) 522-1885 FAX
WWW.NDIA.ORG/MEETINGS/9860

2009 BIOMETRICS CONFERENCE

TO REGISTER, VISIT:
WWW.NDIA.ORG/MEETINGS/9860

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION
STRENGTH THROUGH INDUSTRY & TECHNOLOGY

PROMOTING NATIONAL SECURITY SINCE 1919

2009 BIOMETRICS CONFERENCE

"Strategies For Implementing HSPD - 24"

JANUARY 27-28, 2009
WWW.NDIA.ORG/MEETINGS/9860

SHERATON NATIONAL HOTEL ▶ ARLINGTON, VA

EVENT #9860

Command, Control and Interoperability

Dr. David Boyd
Director
Command, Control and Interoperability
Science and Technology Directorate
U.S. Department of Homeland Security
January 28, 2009

Homeland Security

Command, Control and Interoperability

Mission

Through a practitioner-driven approach, the Command, Control and Interoperability Division (CID) creates and deploys information resources to enable seamless and secure interactions among homeland security stakeholders.




Vision

Stakeholders have comprehensive, real-time, and relevant information to create and maintain a secure and safe Nation.

Homeland Security

Communications Challenge on the Frontlines

Emergency responders—police officers, fire personnel, and emergency medical services (EMS)—need to share vital data and voice information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies.

Responders often cannot talk to some parts of their own agencies—let alone across cities, counties, and states. Ineffective communications risk the lives of responders in the field and can mean the difference between life and death for those awaiting help.

Homeland Security

Command, Control and Interoperability

Information

Identify

Communicate

Manage

Visualize

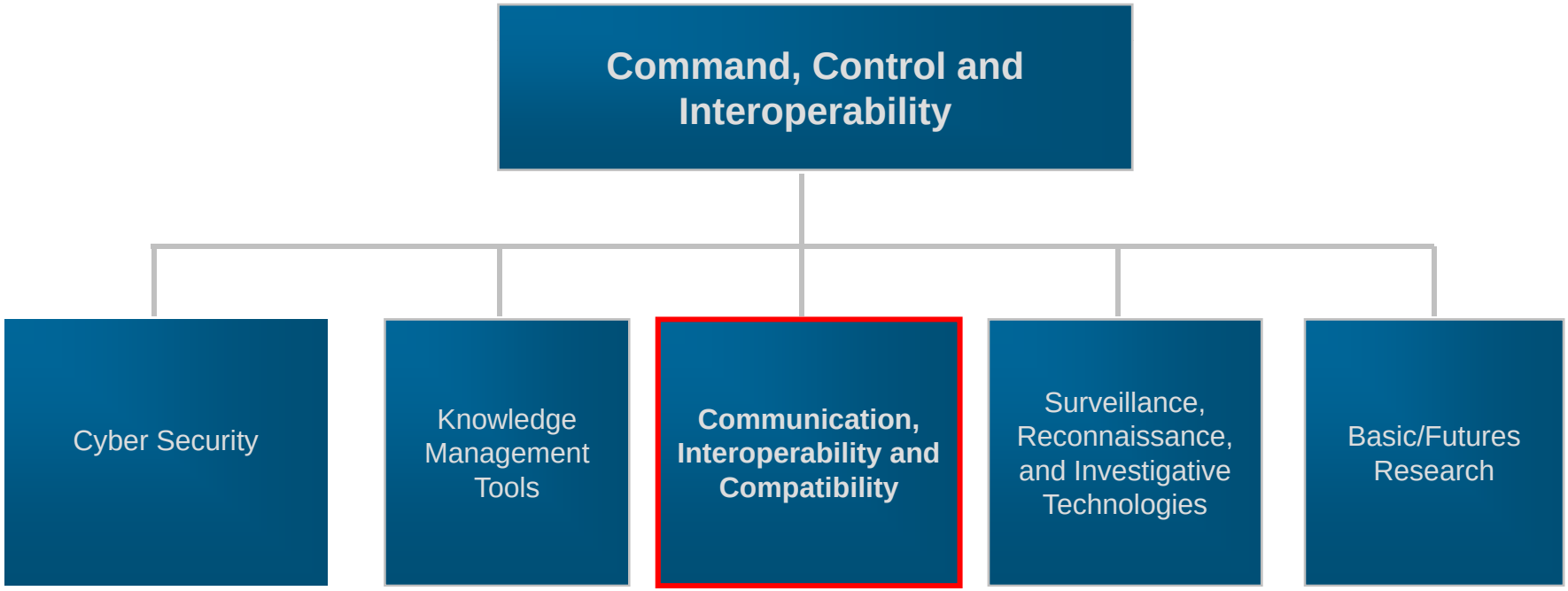
Analyze

Protect

Homeland Security

Command, Control and Interoperability

Through a practitioner-driven approach, the Command, Control and Interoperability Division creates and deploys information resources to enable seamless and secure interactions among homeland security stakeholders. With its Federal partners, the Division is working to strengthen communications interoperability, improve Internet security and integrity, and accelerate the development of automated capabilities to help identify potential national threats.



Why Interoperability Fails

- Locals have almost all the information
- State and Federal agencies need it
- State and Federal direct structures that feed their needs
- State and Federal usually offer litte or no value added or incentive to locals
- So, sovereign locals don’t play
- ***And they rarely need to***

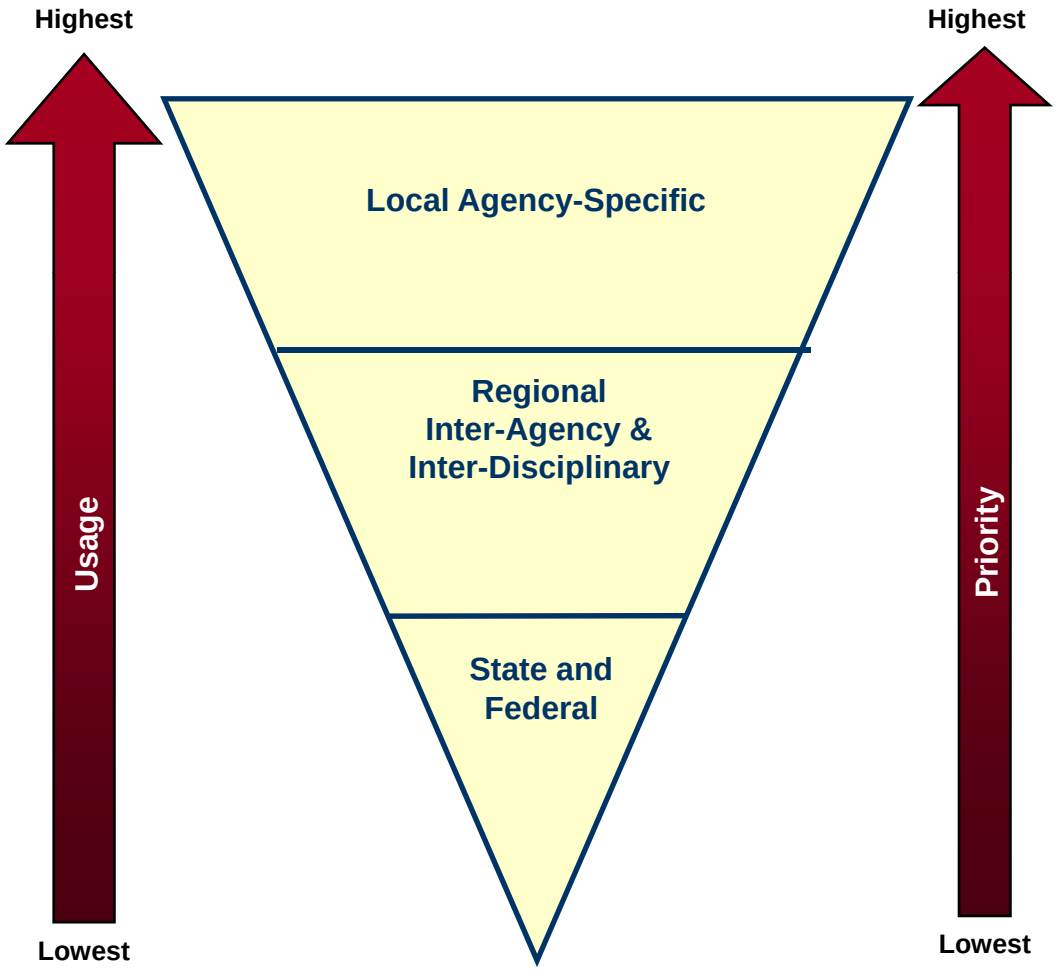
Practitioner-Driven Approach

- A successful strategy for improving interoperability and information sharing must be based on user needs and driven from the bottom up.

- OIC advocates a unique, practitioner-driven governance structure.

- The approach benefits from the critical input of the emergency response community and from local, tribal, state, and Federal policy makers and leaders.

- The approach ensures that resources are aligned with user needs.



Homeland Security

Locals Know

- They have most of the biometric information (fingerprints, etc.)
- Most criminals are local, so they search outward
- More than 95% reside within the state
- Nearly all the rest in adjacent states
- Federal data bases are often last – if at all
- So the key is to incentivize locals – we need them more than they need us

Current Initiatives

Systems Management

Interoperability of Systems

Open Platforms for Emergency Networks (OPEN):

• A supporting infrastructure that allows emergency managers to share incident information regardless of system when using standards-compliant products.

Managing Day-To-Day Information

National Information Exchange Model (NIEM):

• An updated Emergency Management (EM) Domain that allows OIC and NIEM to provide emergency response practitioners with the latest data exchange capabilities for emergency operations. OIC is integrating the Common Alerting Protocol (CAP) and the Emergency Data Exchange Language (EDXL) Distribution Element (DE) data messaging standards into the NIEM EM domain in order to reduce the time and resources required for practitioners to exchange information.

Homeland Security

Acceleration of Standards

The acceleration of standards is a key component of both data and voice interoperability.

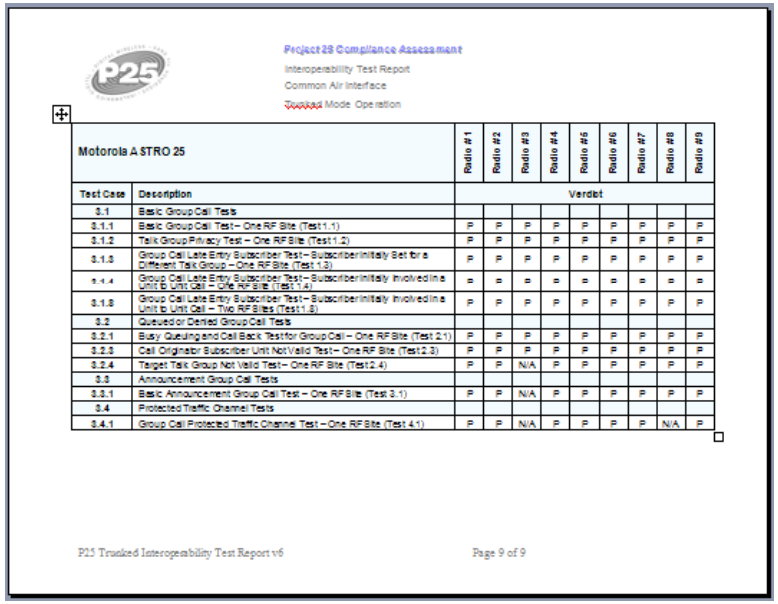
- **OIC supports the acceleration of Project 25 (P25) standards that produce equipment that is interoperable and compatible regardless of the manufacturer. P25 is a suite of eight standards intended to help produce interoperable and compatible equipment.**
- **At the request of Congress, OIC is working with ITS, NIST, the Department of Justice, and the P25 Steering Committee to develop and implement a Compliance Assessment Program (CAP). The Program will validate that P25-standardized systems are P25-compliant and that equipment from different manufacturers can interoperate.**
- **OIC also leads the Information Exchange Standards Initiative, a public-private partnership to create messaging standards to share information between disparate incident management systems and software applications.**

Homeland Security

Project 25 Compliance Assessment

- **Labs are assessed by independent parties prior to being recognized for participation by DHS.**
- **Labs assess/validate equipment as being P25-compliant.**
- **Upon validation, manufacturers declare equipment P25-compliant and submit a Summary Test Report reflecting test results.**
- **An independent Governing Board (GB) represents the collective interests of buyers, sets Program policies, and assists in the administration of P25 CAP.**

Summary Test Report



Project 25 Compliance Assessment
Interoperability Test Report
Common Air Interface
Trunked Mode Operation

Motorola ASTRO 25		Radio #1	Radio #2	Radio #3	Radio #4	Radio #5	Radio #6	Radio #7	Radio #8	Radio #9
Test Case	Description	Verdict								
3.1	Basic Group Call Tests									
3.1.1	Basic Group Call Test – One RF Site (Test 1.1)	P	P	P	P	P	P	P	P	P
3.1.2	Talk Group Privacy Test – One RF Site (Test 1.2)	P	P	P	P	P	P	P	P	P
3.1.3	Group Call Late Entry Subscriber Test – Subscriber Initially Set for a Different Talk Group – One RF Site (Test 1.3)	P	P	P	P	P	P	P	P	P
3.1.4	Group Call Late Entry Subscriber Test – Subscriber Initially Involved in a Unit to Unit Call – One RF Site (Test 1.4)	P	P	P	P	P	P	P	P	P
3.1.5	Group Call Late Entry Subscriber Test – Subscriber Initially Involved in a Unit to Unit Call – Two RF Sites (Test 1.5)	P	P	P	P	P	P	P	P	P
3.2	Queued or Denied Group Call Tests									
3.2.1	Busy Queuing and Call Back Test for Group Call – One RF Site (Test 2.1)	P	P	P	P	P	P	P	P	P
3.2.3	Call Originator Subscriber Unit Not Valid Test – One RF Site (Test 2.3)	P	P	P	P	P	P	P	P	P
3.2.4	Target Talk Group Not Valid Test – One RF Site (Test 2.4)	P	P	N/A	P	P	P	P	P	P
3.3	Announcement Group Call Tests									
3.3.1	Basic Announcement Group Call Test – One RF Site (Test 3.1)	P	P	N/A	P	P	P	P	P	P
3.4	Protected Traffic Channel Tests									
3.4.1	Group Call Protected Traffic Channel Test – One RF Site (Test 4.1)	P	P	N/A	P	P	P	P	N/A	P

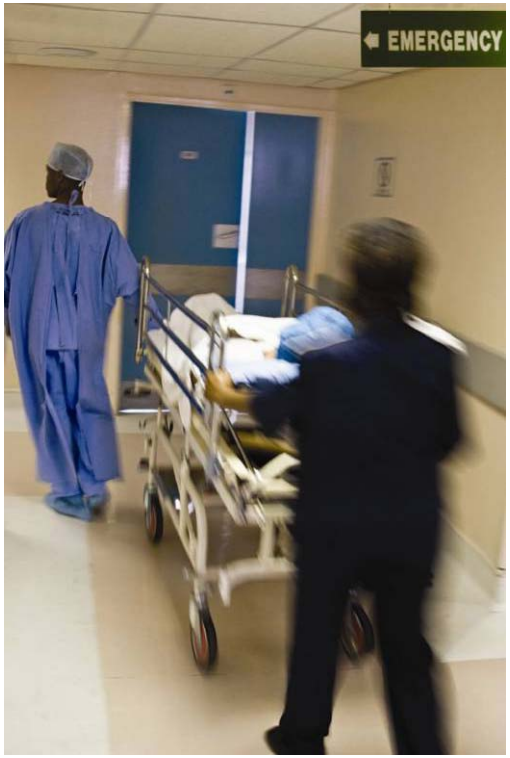
P25 Trunked Interoperability Test Report v6 Page 9 of 9

Provides 'at-a-glance' summary reviews of test results

Data Messaging Standards

- **Data messaging standards enable emergency responders to share critical data—such as a map, a situational report, or an alert—seamlessly across disparate software applications, devices, and systems.**

- **OIC is supporting the development and implementation of the following data messaging standards:**
  - **Common Alerting Protocol Standard**
  - **Distribution Element Standard**
  - **Hospital Availability Exchange Standards**
  - **Resource Messaging Standards**
  - **Situational Reporting Standard**



Homeland Security

Data Messaging Standards

- **Hospital Availability Exchange Standards (HAVE)**

  EDXL-HAVE standard enables responders to exchange information about a hospital's capacity and bed availability with medical and health organizations and others.

- **Resource Messaging Standards (RM)**

  EDXL-RM standard enables responders to exchange resource data for operations, including emergency response personnel and equipment. This information sharing standard will improve emergency preparedness, response, and recovery efforts.

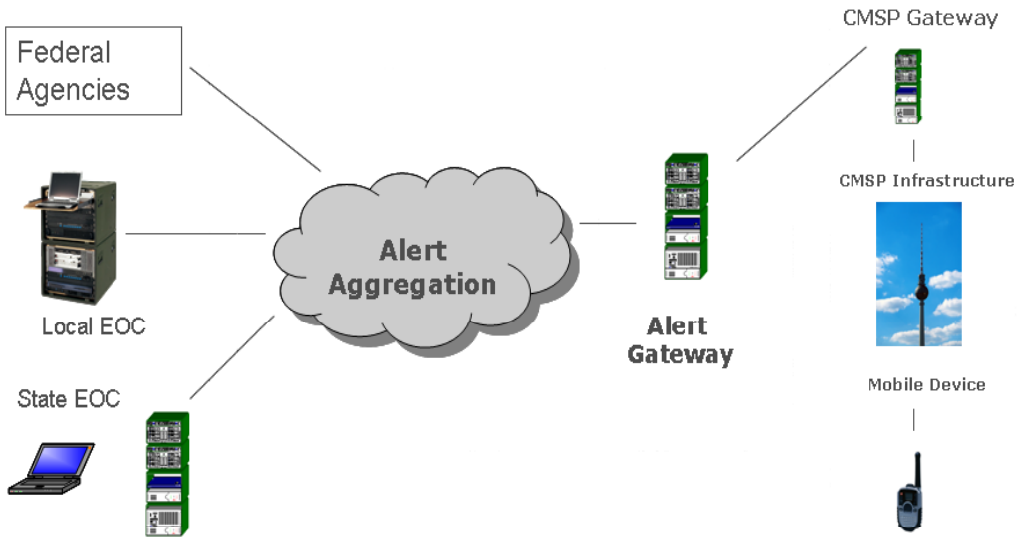
Homeland Security

Commercial Mobile Alert Service (CMAS)

- The **Warning, Alert, and Response Network** (**WARN**) **Act** of 2006 established the **Commercial Mobile Alert Service** (CMAS) to provide emergency alerts to mobile devices. Since over **80 percent of the American population** subscribes to wireless service, this represents significant progress toward a more comprehensive capability to alert people of threats where they are.
- CID owns the **Research, development, testing, and evaluation** (RDT&E) portion of CMAS. Using recommendations from subject matter expertise pooled by the FCC as a starting point, CID's program supports partners to **leverage current technologies while influencing future technologies** in order to increase the number of commercial mobile service devices that can receive emergency alerts.

Major challenges addressed by CMAS:

- **Relevance** of alert based on geographic **location**, **imminence** of threat, native **language**, and **accessibility** of information.
- **Authenticated** origination of alerts that are **meaningful**, **integrated** into a **secure** National infrastructure, and delivered in a **timely** fashion.
- Social science aspects of the **public response** to alerts received on mobile devices, including **public education** and **network use.**



Homeland Security

CIIMS

- **The Critical Infrastructure Inspection Management System (CIIMS) is a new aerial technology that will enable police flight crews to more efficiently manage inspections of important structures such as dams, bridges, large industrial complexes, and urban areas.**

- **A cost effective technology—the hardware package has a current price tag of $3,000—CIIMS enables aviation crews to complete aerial inspections more quickly and efficiently.**

- **For each site, the CIIMS computer uses photographs, geographic coordinates, and inspection questions intended to address the location's security. Flight crews use the system to inspect the site and forward observations to homeland security partners on the ground.**

- **CID is piloting CIIMS in partnership with the Maryland State Police and Los Angeles Police Department.**

- **Readily transferable, CIIMS can assist other state and Federal agencies in their efforts to secure critical infrastructures and resources nationwide.**

Homeland Security

Slide 16

J1 I just edited the slide to reflect new partnership with LAPD also. (added lapd to 4th bullet, took out state police, added 'urban areas' to first bullet)

Jayme.McKinley, 10/6/2008

Homeland Security

NDIA Policy Panel

Thomas E. Bush, III
Assistant Director,
Federal Bureau of Investigation
Criminal Justice Information Services Division
(CJIS)

CJIS Background

- Supports criminal and noncriminal justice agencies through sharing of biometric and biographic data
- Data collected by federal, state, local and tribal law enforcement; managed through shared management process
- Privacy and security issues addressed through several processes
- CJIS continues to be on the forefront in identity-management systems development

HSPD-24

- Desired end-state:
  - Continue to expand biometric collection, retention and dissemination capabilities beyond fingerprints through the FBI's Next Generation Identification
  - Expand Biometric Interoperability efforts beyond the sharing of fingerprint data to DHS to include other modalities and agencies
  - Further relations with our foreign partners through our FBI LEGAT offices to obtain biometric, as well as biographic and contextual information on persons posing a threat to US interests or persons
- Implementation of HSPD-24 remains a work in progress

HSPD-24

Known or Suspected Terrorists (KST)

- FBI has fully supported the sharing of KST data with other agencies in accordance with HSPD-6, HSPD-11 and HSPD-24
  - Close coordination with TSC and DOS (with FBI LEGAT offices)
  - CJIS Division Intelligence Group: created to exploit information contained in CJIS systems for dissemination to our customers
  - Supports efforts of the Biometrics Interagency Coordination Group in implementing the KST Framework – “Biometric Framework to Support Counterterrorism Efforts”

HSPD-24

National Security Threats (NST)

- Currently there is no government-wide policy that defines NST
  - HSPD-24 Action Plan recommended the creation of an inter-agency working group to determine NST categories and sharing mechanism
  - The NST Implementation Working Group convened in December and is co-chaired by the FBI and ODNI

SEGOB

SECRETARÍA DE GOBERNACIÓN

National Population Registry and Personal Identification

NDIA 2009 BIOMETRICS CONFERENCE
"Strategies for Implementing HSPD-24"

International Panel

Carlos R. Anaya Moreno
National Register of Population and Personal Identification
Mexico

Arlington, Va.
January 28, 2009

-DRAFT Version- January 16, 2009

SEGOB

SECRETARÍA DE GOBERNACIÓN

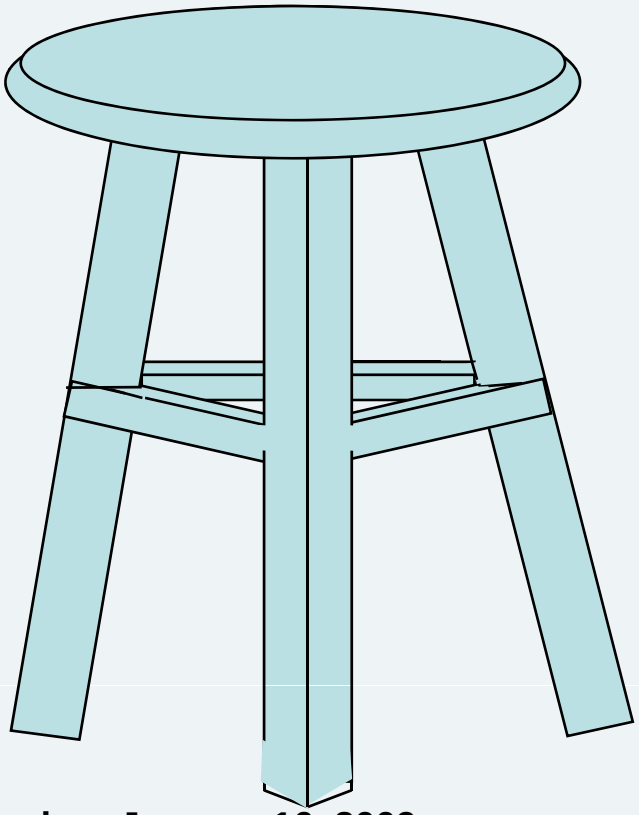
National Population Registry and Personal Identification

Identity Service Mission

Register and credit the identity of the people to offer the Personal Identification Service.

-DRAFT Version- January 16, 2009

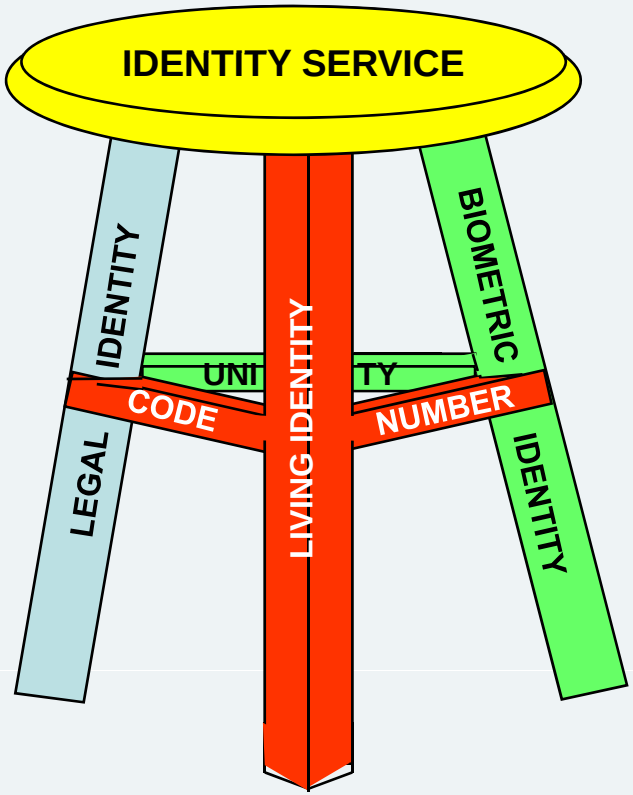
Identity Service



Lets start with an allegory

This chair projects stability

It is structurally integrated by:
Three legs
Three supports
One Platform



An Identity Service based in three types of identity delivers Security and Trust

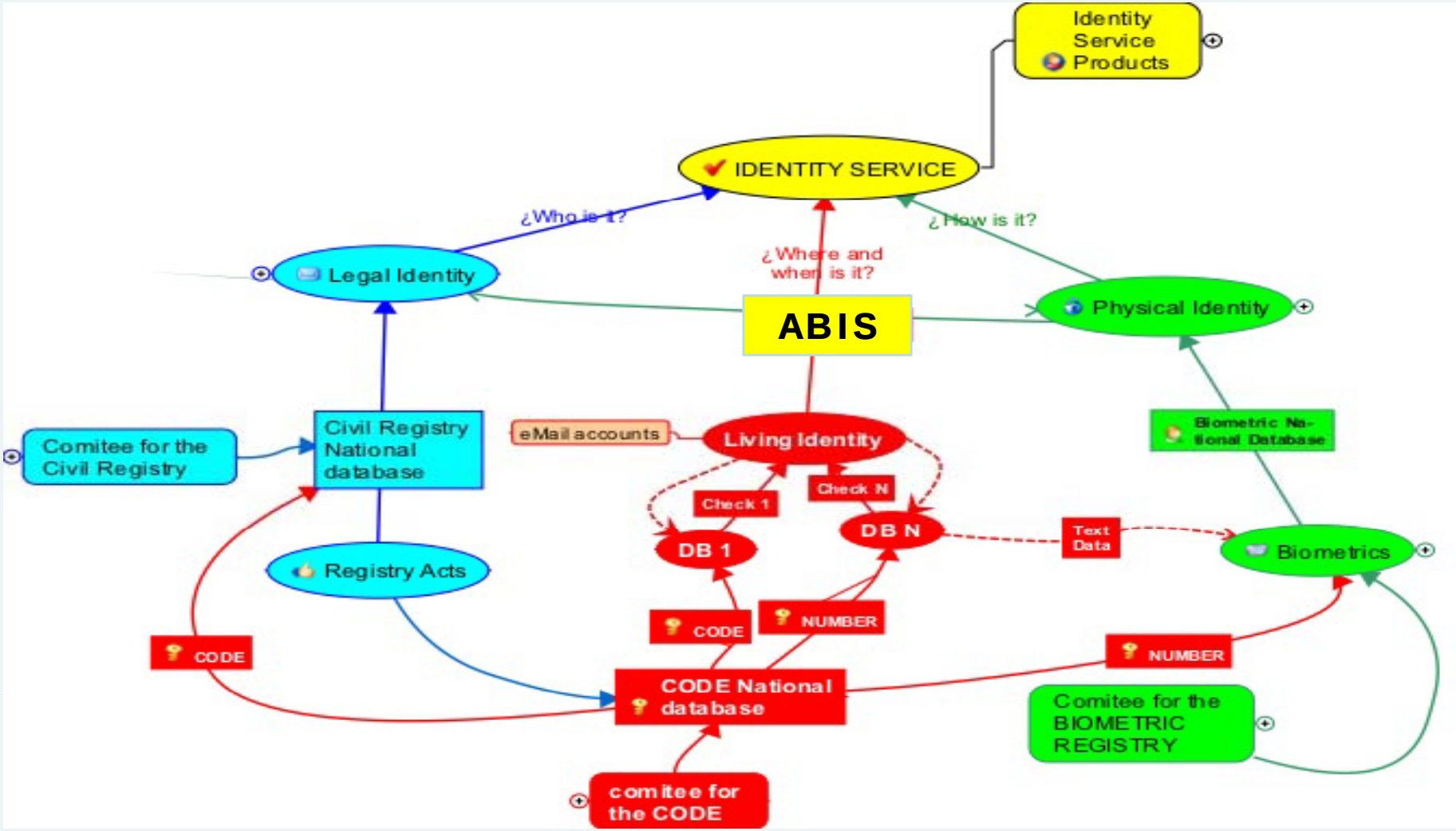
The three legs are:
Legal Identity
Living Identity
Physical Identity

It has three supports:
Number
Code
Unity

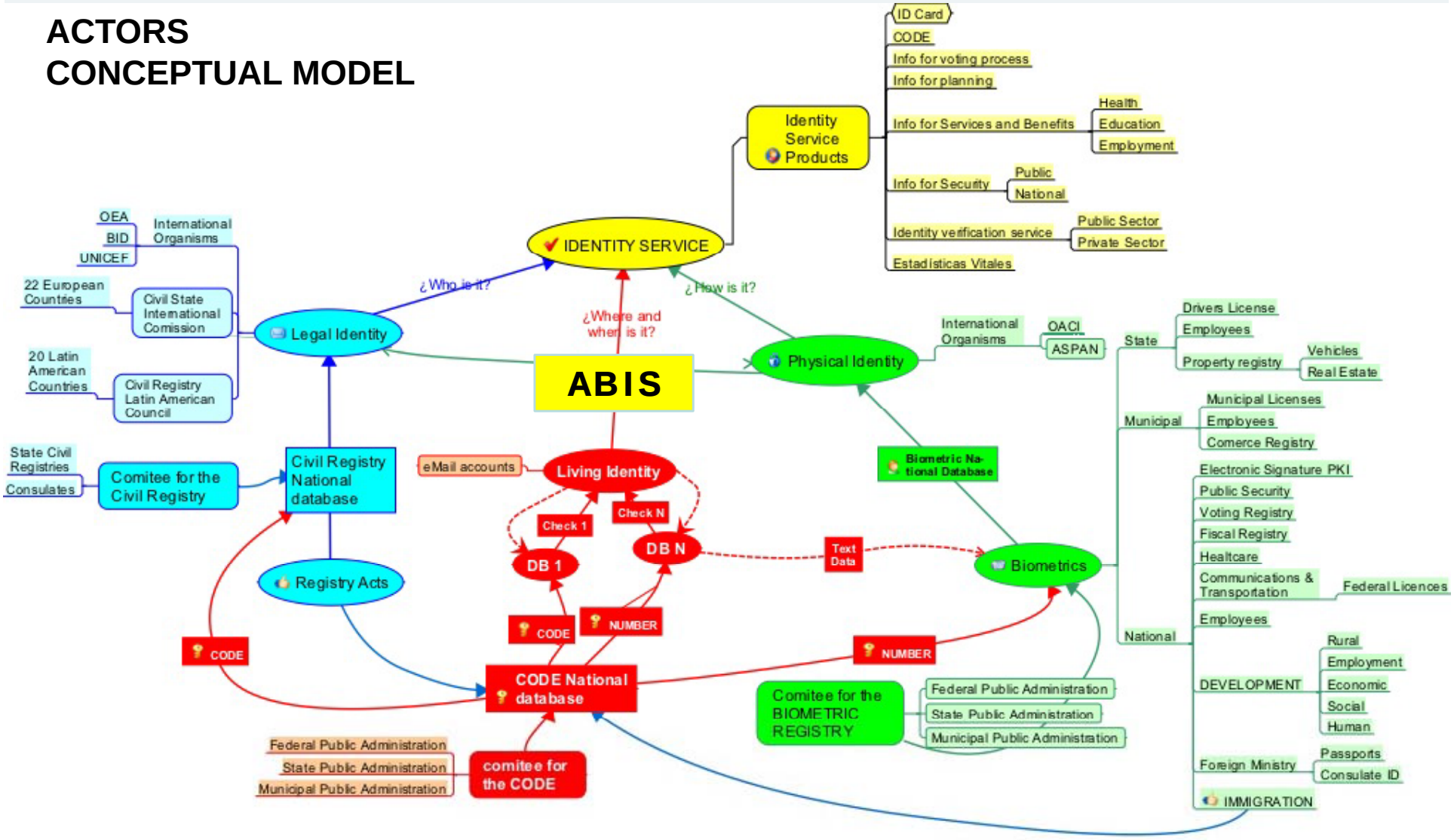
And one platform:
Identity Service

-DRAFT Version- January 16, 2009

CONCEPTUAL MODEL

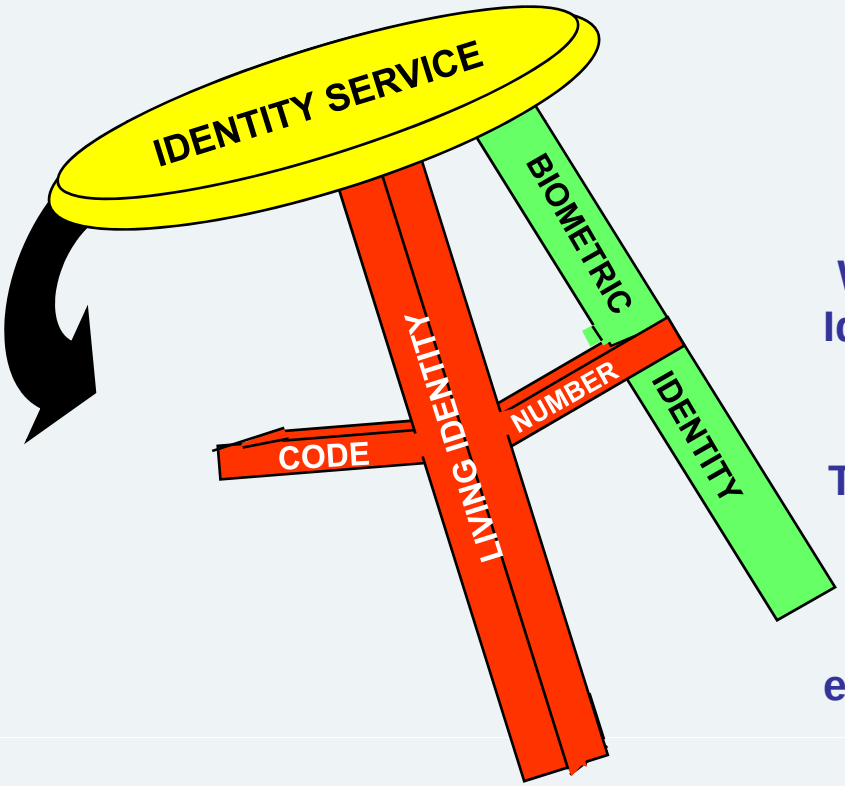


ACTORS CONCEPTUAL MODEL



Using this allegory we will analyze the variations on the structural design of the Identity Service that are applied

-DRAFT Version- January 16, 2009

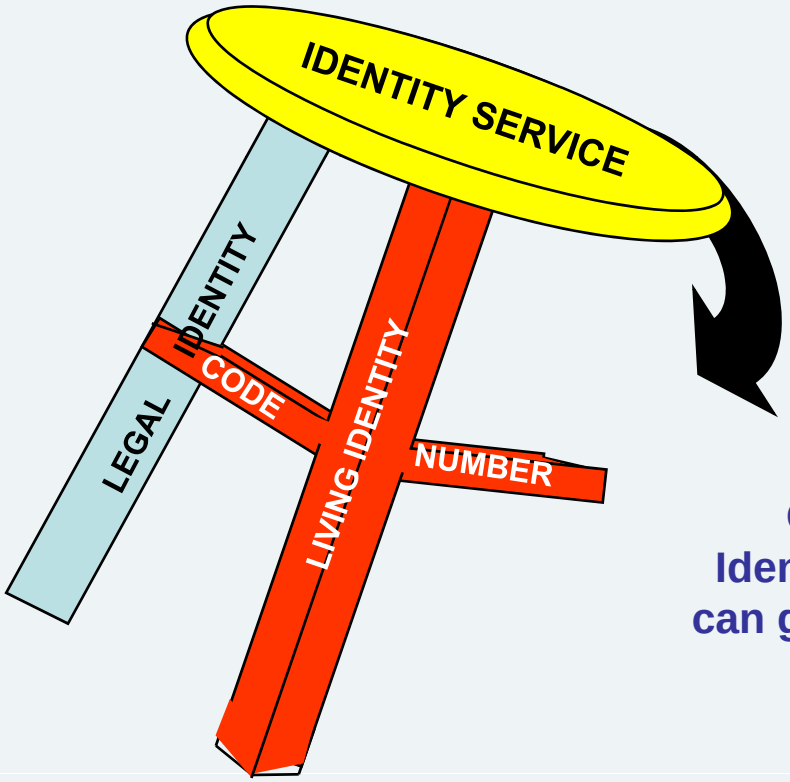


When the Identity Service lacks the Legal Identity it becomes weak and wont deliver Security and Trust

This happens with some Identity Services that are based on "Good Will"

Some examples are those that are used exclusively for voting or for police control

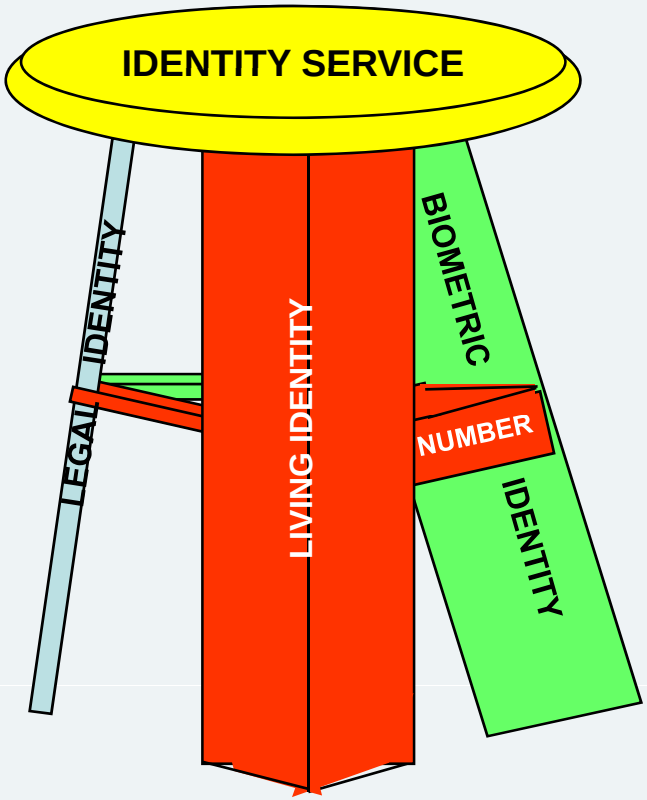
-DRAFT Version- January 16, 2009



When the Identity Service lacks Physical Identity it allows identity fraud, multiple identities and changeable identities

Outside of very few exceptions, most of the Identity Services don't have Unity services that can guarantee the Physical Identity linked to the Legal Identity

-DRAFT Version- January 16, 2009

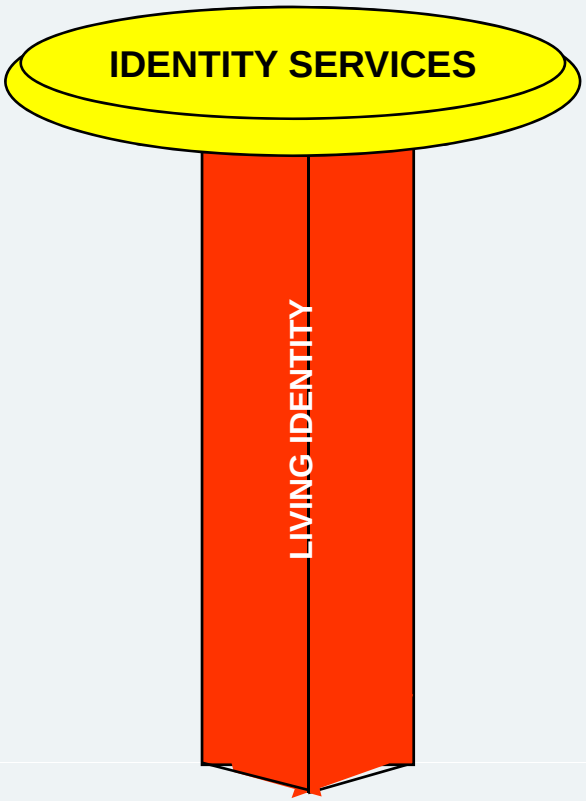


When the Living and Physical Identities grow rapidly within the Identity Service, the Legal Identity debilitates itself until it breaks along with the lateral supports of code and unity, making vulnerable the personal data confidentiality (privacy) and with it the legal security and the citizens trust

This happens when resources are allocated only for "Criminal" Identity Systems

With this vision, the result is that "Civil Identity" systems are prevented of creating a climate of trust that is indispensable for the development, as well as restricting the huge benefits of crime prevention that the civil systems allow

-DRAFT Version- January 16, 2009



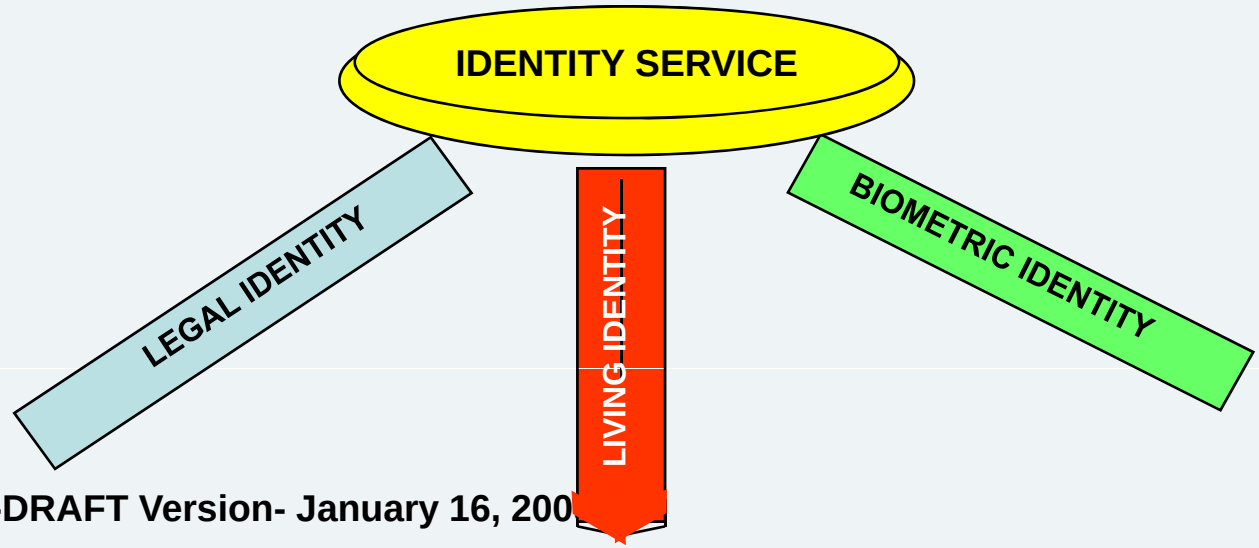
When in the Identity Service the Living Identity grows immeasurably, the other identities are reduced, making vulnerable the personal data confidentiality ,the legal security and the citizens trust.

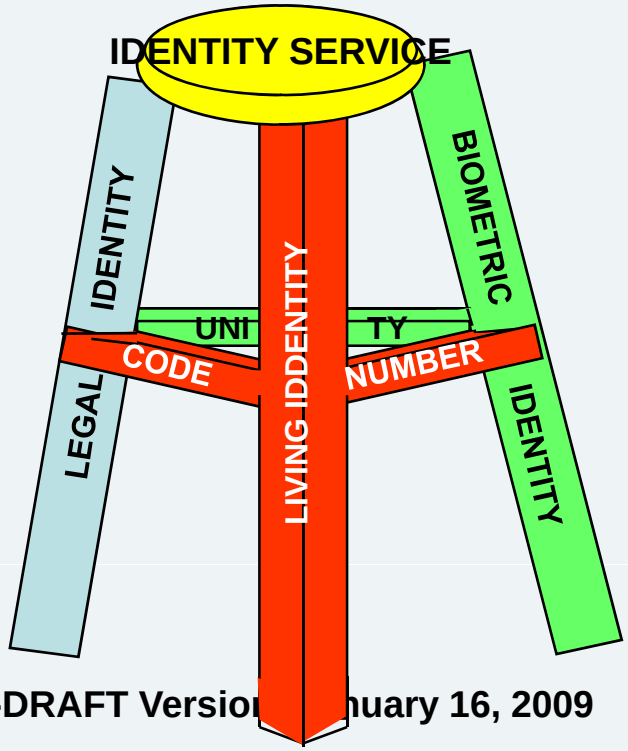
This happens when the Identity Service is sold by the Private Sector without the intervention or audit of the Public Sector.

-DRAFT Version- January 16, 2009

An Identity Service without lateral supports, even tough it has the three type of identity united at the top, it won't hold the weight of the service and will collapse.

This is likely in some identity services where even though they have the Legal, Living and Physical Identities, there are no Unique Codes and an Identity Service that can guarantee a unique relationship between a person and a record resulting in the inability to provide the security needed to establish a persons Identity because in practice there are three separated services.





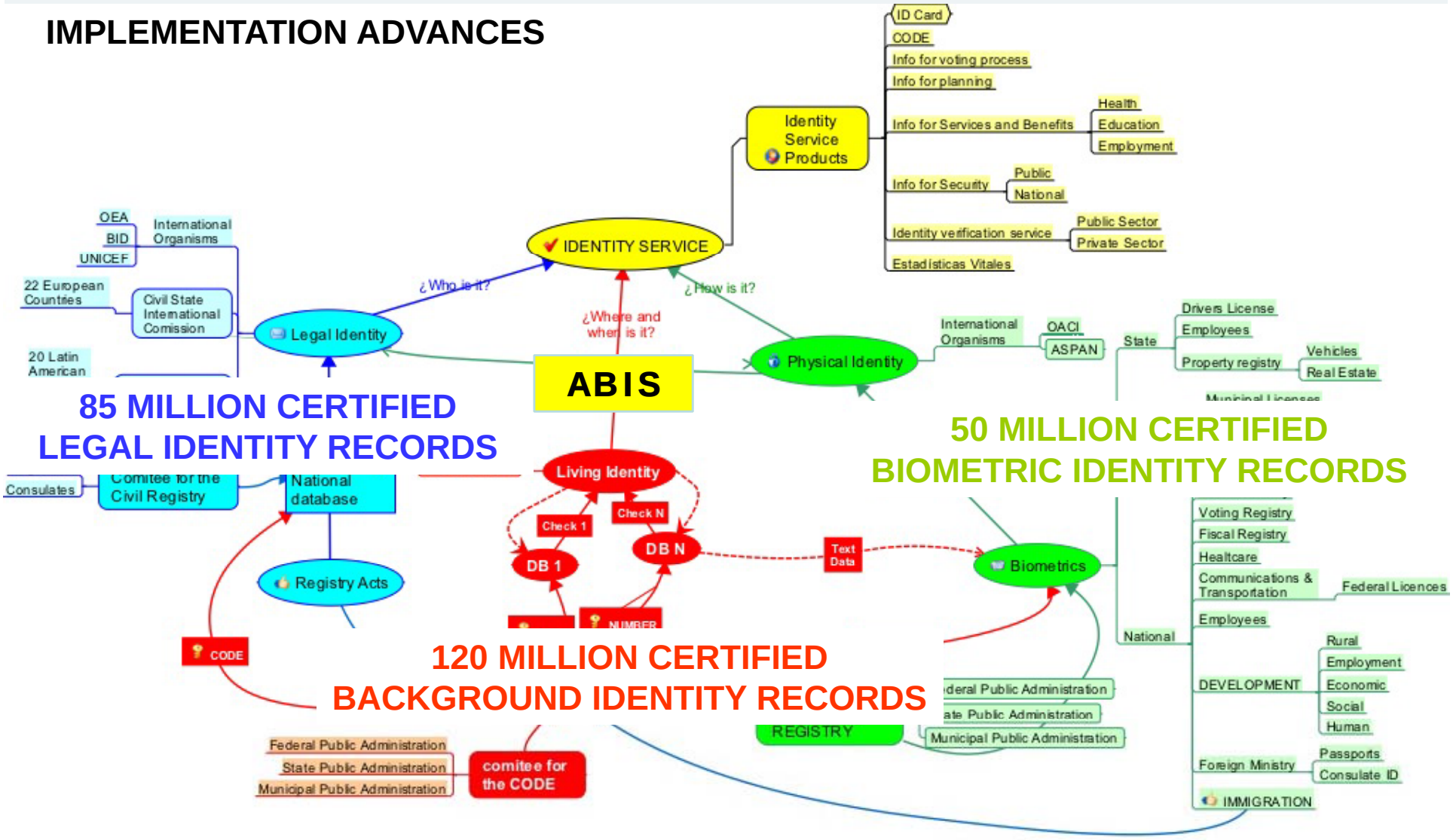
-DRAFT Versio nuary 16, 2009

An Identity Service that even tough it is supported by the three types of Identities and that it has the three lateral supports, if it has a small Platform (objective) results in a very uncomfortable system because of its costs and inefficiency, as well as being unable to provide the benefits that are required of it.

This problem is present when the Identity Services have been structured with the sole purpose of creating voting instruments or taking into account Public or National Security

Even worse are the Identity Services created exclusively for political or social control because instead of guaranteeing the "Right to Identity", they violate Human Rights and privacy laws.

IMPLEMENTATION ADVANCES

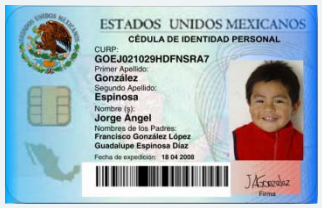


Objectives

- Guarantee the **Right to the Identity**.
- Certify Mexican **citizenship** (Mexican Constitution, 36 Article).
- Comply with the Universal Declaration of **Human Rights** (Article 6).
- Strengthen the person's **management capacity.**
- **Simplify and reduce procedures .**
- Support **full access** of Mexico to the **New Information Society.**
- Grant **certainty to the economic and social sectors** through a document that reliably certifies identity. This will help to generate trust in commercial and financial activities.

- The **National Population Registry**, is a **service of public interest offered by the Mexican State**, and it certifies the identity of the persons who conform the mexican population.
- **The Identity Card will be issued to reliably certify the identity of the person**, and it will be recognized by the authorities in Mexico and abroad, as well as by natural and moral persons.

CURP

- **National Registry of Citizens** →  **Citizenship Identity Card**
- **Minors Registry** →  **Personal Identity Card**
- **Foreigners Catalogue** →  **Migratory Form (INAMI)**

SEGOB

SECRETARÍA DE GOBERNACIÓN

National Population Registry and Personal Identification

Mexican ID Card (Sample)

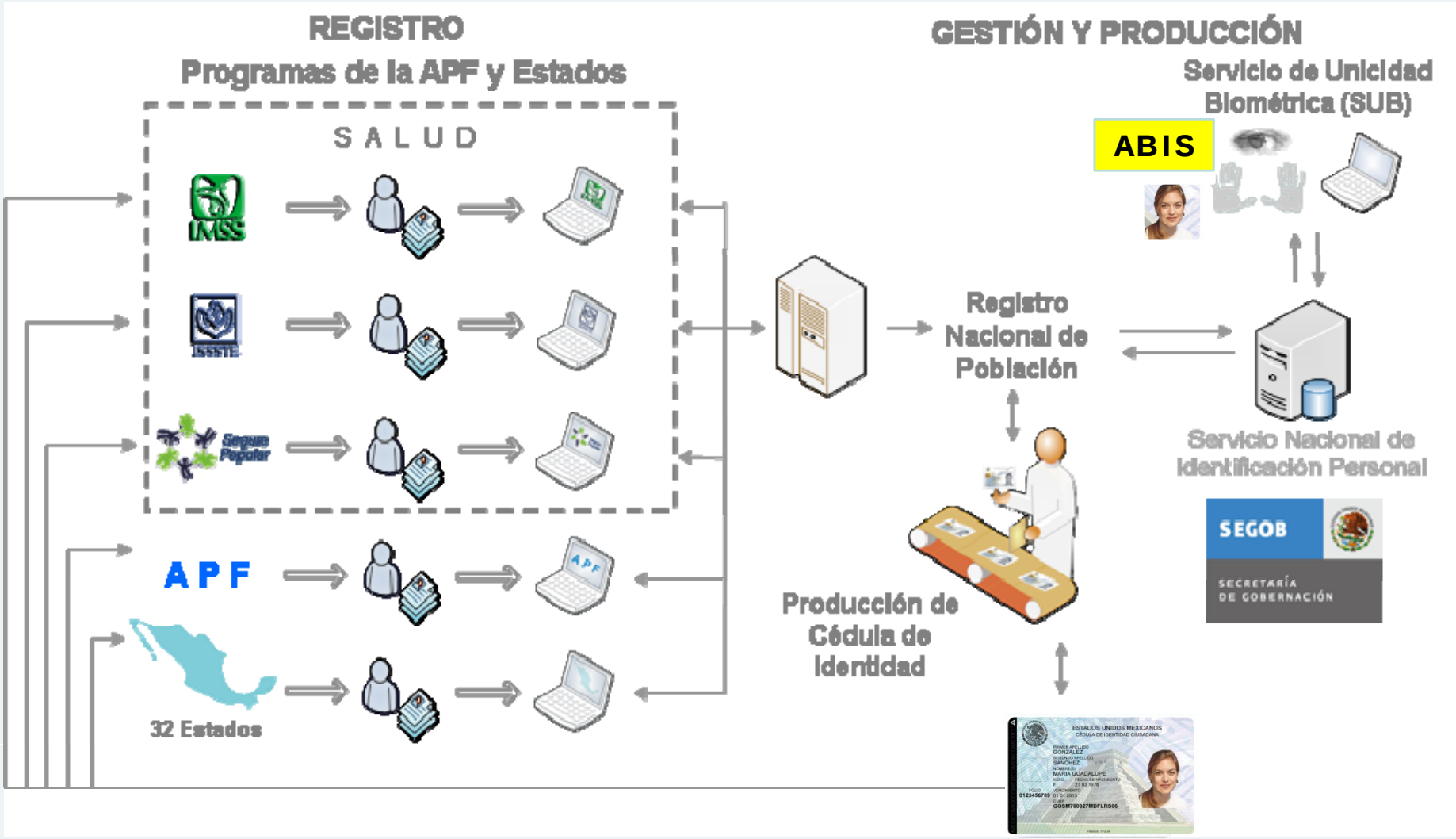
DEPLOYMENT OF 100 MILLION ISO/ICAO COMPLIANT ID CARDS IN 5 YEARS. 80 MILLION IN THE FIRST 3 YEARS.

-DRAFT Version- January 16, 2009

SEGOB

SECRETARÍA DE GOBERNACIÓN

National Population Registry and Personal Identification



-DRAFT Version- January 16, 2009

ANSI NCITS 322
ISO/IEC 10373
ISO/IEC 7810 ID-1.
ISO-7816-1
ISO-7816-2
ISO-7816-3
ISO-7816-4
ISO-7816-5
ISO/IEC FCD 19794-5 Part 5.
Doc 9303 Part 3 ICAO Travel documents.

CONSIDERATIONS OF THE MEXICAN IDENTIFICATION SERVICE

- Civil Registry is the Oldest Identity Service, whit more than 150 years.
- It credits the Legal Identity, fundamental to the other identities
- It has de legal capacity to give “Public right of the persons identity”
- By definition it is a Public Registry, which enables that the personal identity “Who am I” becomes a public element, which is not the case for the rest of the personal information: “Where I live”, “How much is my income”, “Where I work”, etc. that are private elements.
- It’s the fundament for the “Identity Right”.

-DRAFT Version- January 16, 2009

Basic considerations to guarantee the "Identity Right"

- Gratuity of birth registry.
- Gratuity of Identity Document.
- Modernization of the Civil Registry.
- Implementation of IT.
- Establishment of Population Registry Unique Code.
- Establishment of mobile enrollment stations to be able to get to the farthest regions of the country and reduce the under registry.
- Civil registry units in hospitals and health centers.
- Out of time registry campaigns.
- International collaboration for the registry of immigrants.
- Interchange of Best Practices in the international level.

People are NOT transactions

We have to break the “Transactional Paradox” of database processing and retake the concept of Public Service, respecting the dignity of the people and there right to privacy.

It's absurd that in the Public Registry the records are tracked by type of act, even at the database level, and not by the persons identity, who we serve.

It is also absurd that the “identities” are repeated as many times as levels of the government that serve a person (federal, state and county), requesting the person to credit there identity every time in every level and office.

We have to put the person at the center and create a New Paradigm related to Public Service, “One Person, One Government”.

-DRAFT Version- January 16, 2009

Identity Verifications links:

For Documental Identity

http://www.gobernacion.gob.mx/CurpPS_HTML/jsp/CurpTDP.html
http://www.e-mexico.gob.mx/wb2/eMex/eMex_Consulta_tu_CURP
http://www.sre.gob.mx/

http://www.renapo.gob.mx

80 portals whit 500,000 daily transactions.
And another 100,000 daily transaction whit web services.

For Biometric Identity

http://148.245.141.196/

-DRAFT Version- January 16, 2009

THANK YOU VERY MUCH

Carlos R. Anaya Moreno

cranayam@segob.gob.mx

-DRAFT Version- January 16, 2009

NDIA
Government Panel

Ms. Kimberly Del Greco
Federal Bureau of Investigation
Criminal Justice Information Services

Biometrics

- Biometric systems are being used by numerous programs to establish, authenticate and verify identity.

- Each US Government Agency has to meet its own mission
  - Applying existing and emerging biometric technologies to collect, use and share data in identification and screening processes

FBI Programs

- Next Generation Identification
  - Multi-modal
  - Flexible and scalable
- Biometric Interoperability
  - DHS US-VISIT IDENT
  - DOS
  - DOD's ABIS
- BCOE
  - Foster collaboration, improve information sharing, advance biometrics through research and academia.

HSPD - 24

- NSTC partnership with NCTC for Known or Suspected Terrorist (KST) collection, storage, use and sharing biometric and biographic data
- KST framework and business process
- National Security Threat Interagency Working Group – NST IWG
  - NST categories
  - Current processes for sharing and identify gaps

BIOMETRIC VISA PROGRAM

BioVisa & US-VISIT as Partner Programs

- Under BioVisa, DOS started collecting two index fingerprints of visa applicants in September 2003.
- By October 7, 2004, all posts issuing visas were capturing fingerprints of applicants.
- BioVisa has been responsible for thousands of refusals of ineligible applicants who would have likely succeeded in obtaining visas in the past.
- Decision to Transition from two to ten prints was made in 2005.
- Advantages of Ten Prints:
  - Improves accuracy
  - Additional matching opportunities
  - Allows for a check against FBI IAFIS criminal master file.

DoS Facial Recognition System Screens Photos of Visa Applicants

- Photos of all applicants exempt from fingerprinting are screened against a photo watchlist of known or suspected terrorists (KSTs) in the DOS Facial Recognition (FR) System.
- Exemptions from Fingerprinting:
  - Diplomats/certain other government officials.
  - Children under 14 and adults over age 79.

Ten Prints Screened Against KST Latents in IDENT

- In 2007 DOS transitioned all visa-issuing posts from two to ten fingerprints.
- Ten Prints sent to IDENT are checked against all available KST and other criminal latent fingerprints.
- Latent fingerprints collected from improvised explosive devices (IEDs) in Iraq and Afghanistan are transferred to IDENT to be checked against visa applicant fingerprints.

BioVisa Ten Prints Advance IDENT-IAFIS Interoperability

- In January 2008 ten fingerprints of visa applicants began to be searched against IAFIS criminal master file.
- The visa applicant ten prints continue to be sent first to IDENT, which relays them to IAFIS.
- IAFIS results are returned to DOS via the DOS interface with IDENT.

HSPD-24 – Technology Panel

DR. STEVE ELLIOTT

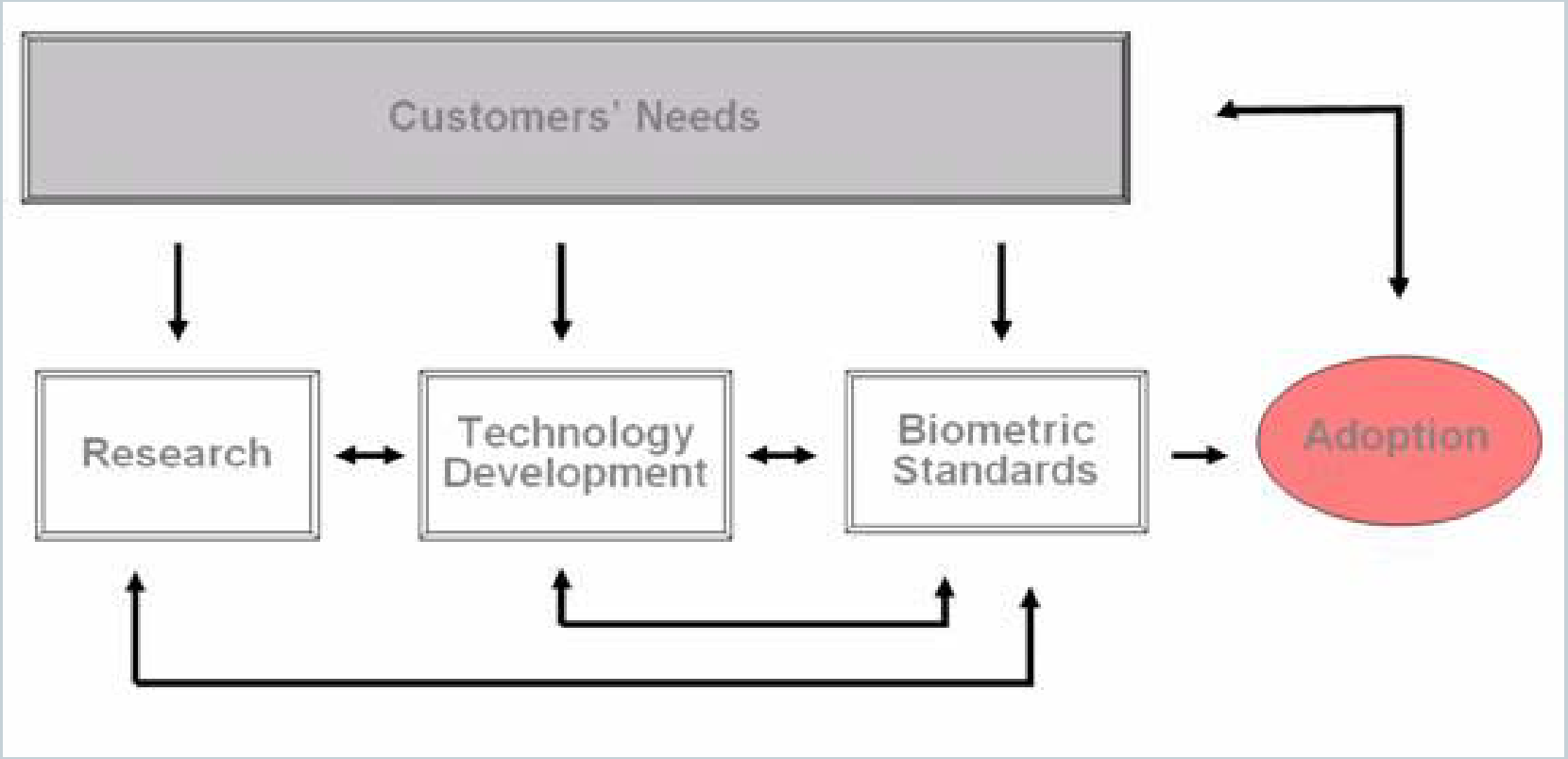
Growth of Government-wide Biometrics Policy

- Executive Order 12881
- HSPD-6
- Executive Order 13354
- HSPD-11
- HSPD-12
- HSPD-15

How can academia help

- Play an active role to meet the challenges associated with government ID management requirements
  - Core R&D
  - Applied R&D
    - Participation on standards
    - Testing and Evaluation of Products
    - Working with certification bodies
    - Training (external and within the curriculum)
    - Testing effectiveness of standards
    - Play an advisory role for those that need to implement standards

Academia and Standards



Interoperability of Fingerprint Sensors

- HSPD 24 highlights the importance of using compatible methods of data collection
- Fingerprint sensors introduce distortions and variations in the images captured by the sensor
- Matching fingerprints collected on different types of sensors increases probability of false accepts and false rejects
- Fingerprints collected at border control might not work well with fingerprints collected on a mobile device in the field

Interoperability

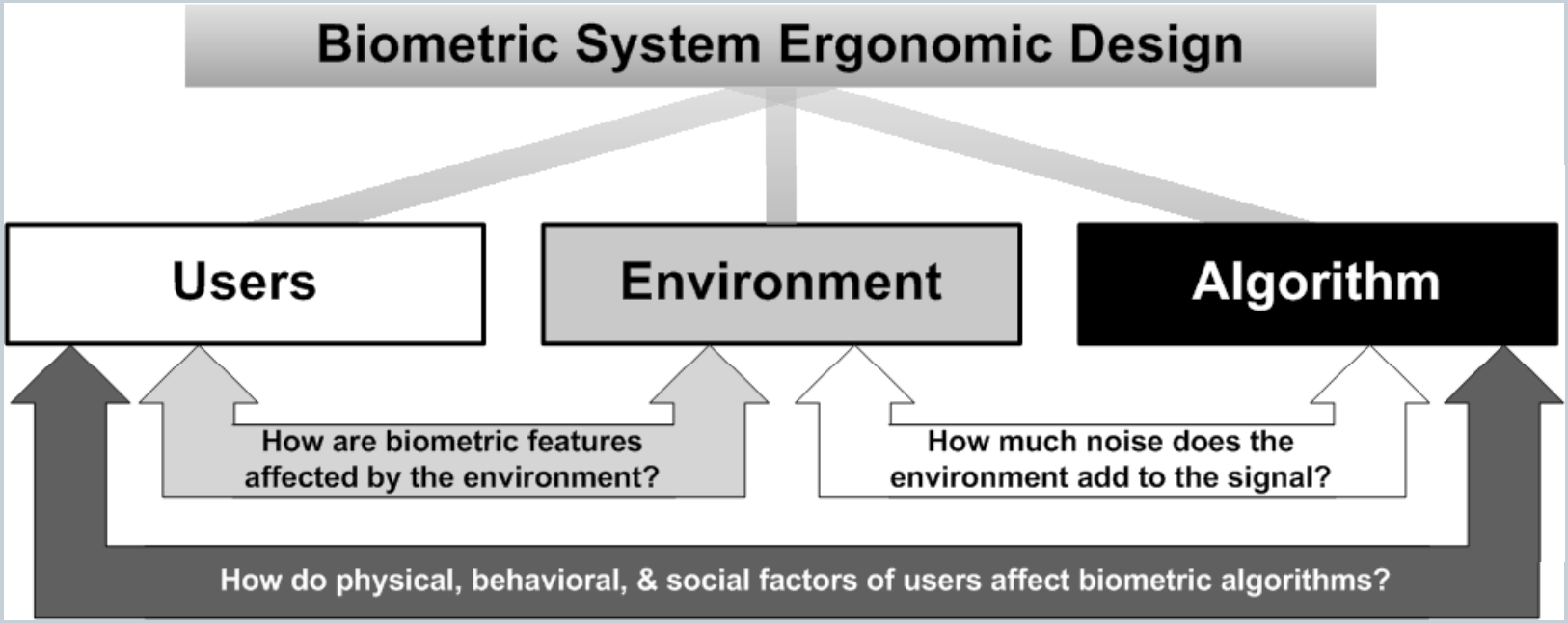
- MINEX Test evaluated interoperability of fingerprint template generators and matchers
- Currently conducting research on statistical testing of interoperability of sensors
- Evaluating a compensation model to remove geometric inconsistencies between fingerprint images

MultiBiometrics

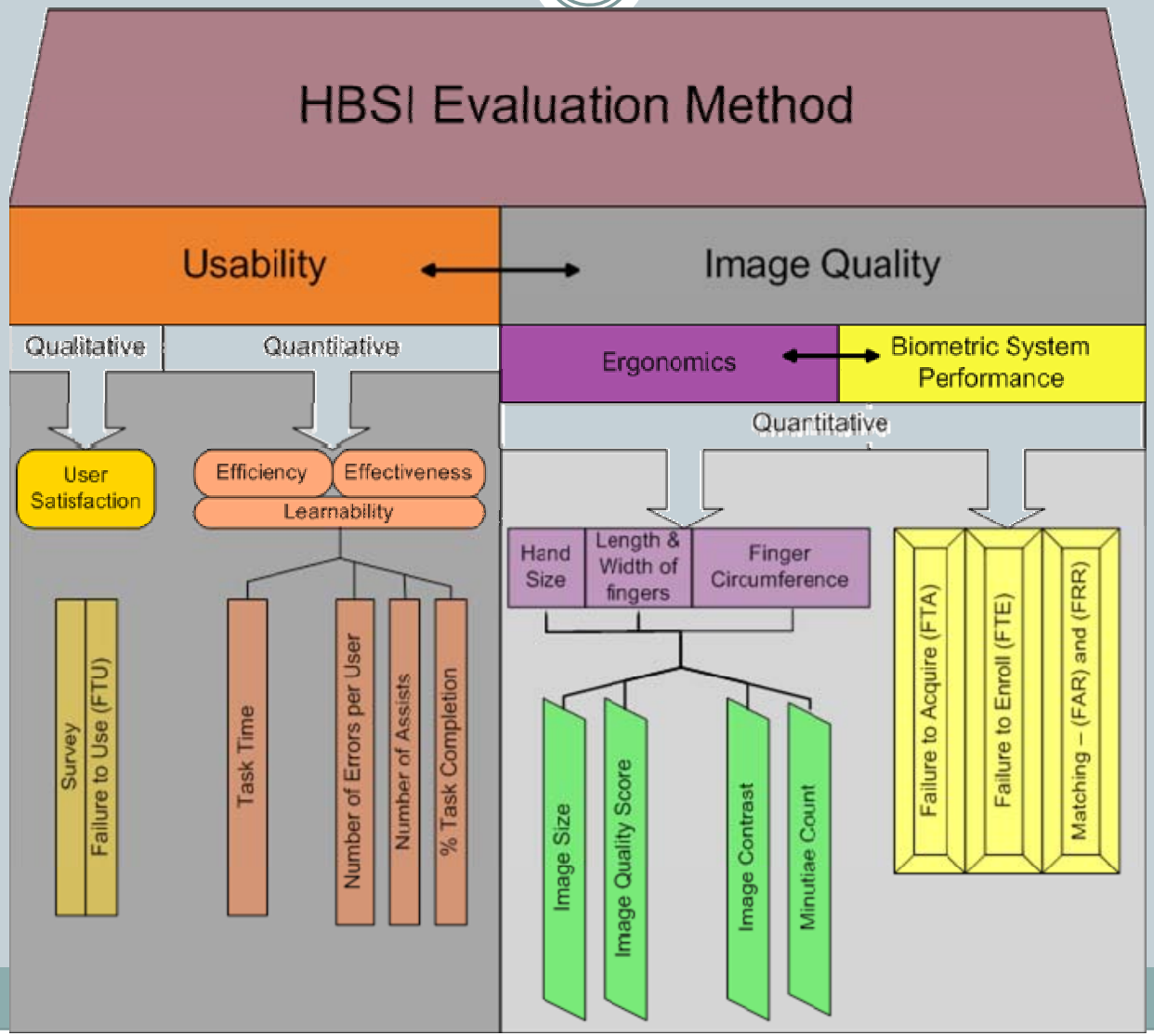
- Next Generation Identification systems will be capable of capturing and storing multiple biometrics
- Key challenge is how to fuse the multiple biometric traits to improve matching ability
- Extend the knowledge of image quality from single modality to impact of quality on multiple modalities

Testing Effectiveness of Standards

- Are standards helping to maintain the matching ability while promoting data exchange, standardized capture methods, and use in multiple applications?
- Large scale tests required to understand the impact of standards (MINEX, IREX)


Biometric System Ergonomic Design
Users
Environment
Algorithm
How are biometric features affected by the environment?
How much noise does the environment add to the signal?
How do physical, behavioral, & social factors of users affect biometric algorithms?

- What impacts the performance of a biometric system?
  - Is the algorithm the cause of matching errors?
  - Is the application/environment the problem?
  - Is the design of the sensor the problem?
  - Are the users the problem?
    - Cannot do what the system/sensor is asking for.
    - Do not understand how to use the system/sensor.
    - Cannot produce repeatable images.


HBSI Evaluation Method
Usability
Image Quality
Qualitative
Quantitative
Ergonomics
Biometric System Performance
Quantitative
User Satisfaction
Efficiency
Effectiveness
Learnability
Survey
Failure to Use (FTU)
Task Time
Number of Errors per User
Number of Assists
% Task Completion
Hand Size
Length & Width of fingers
Finger Circumference
Image Size
Image Quality Score
Image Contrast
Minutiae Count
Failure to Acquire (FTA)
Failure to Enroll (FTE)
Matching – (FAR) and (FRR)

Improving Image Quality

- Image Quality
  - Good image in = good performance
  - How do we get good images???
    - Understanding how the devices work optimally
    - Understand where the data capture “sweet spot” is (mobile iris for example)
    - Improve image quality
    - Change the design of the devices
    - Focus groups of specific populations

Aren't Biometrics Really Just Data?

NDIA Biometrics Conference
January 28th 2009

Paul Garrett

Former (as of 1/20/09)

Department of Justice IT Guy (OCIO)

pgarrett@ashcroftgroupllc.com

All content is the opinion of the speaker and should not be construed as agency policy.

Impediments

In Order of Importance

1. Congress
   - Funding in stovepipes
   - Oversight in stovepipes
2. Agencies
   - Too technical, leave it to the techies
   - Separated from info sharing programs
   - Limitations on legacy systems
3. Programs & Their Contractors
   - My program is better than yours!
4. Technology & Policy Hurdles

Engines are to GE as Biometrics are to DOJ/DHS

GE Aviation
- Commercial
- Business
- Marine
- Military

GE Transportation
- Rail
- Marine
- Mining
- Stationary
- Drilling
- Wind

imagination at work

Competitors:

United (Pratt & Whitney) Yanmar

Cummins Briggs & Stratton

DOJ
- Prosecution/Litigation
- Investigation/Law Enforcement
- Intelligence
- Corrections
- Regulatory
- Program Coordination (Grants)

DHS
- Information Sharing & Analysis
  - Investigation/Law Enforcement
  - Intelligence
- Prevention & Protection
- Preparedness & Response
- Research
- Commerce & Trade
- Travel Security
- Immigration

Competitors:

DOD

NCTC

CIA

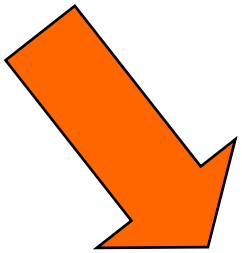
If the next Congress and next Administration do not understand the difference and the different needs……

Others make engines, competition is a good thing in markets, but not necessarily in government.

Importance of NGI

- Potential to serve many USG needs
  - Validating a negative, as important as proving a positive
- CJIS history of service, ability to support long term
  - Universities (WV & Pitt) and Private Sector
  - DOD presence and planned growth
- Procurement designed for the long-term
  - Inclusive procurement but unimpressive showing by other agencies
- CJIS Advisory Policy Board (APB) support

Function Areas



Collection

Matching

Use/Query

Model Applies to:

Watchlist

Bank Secrecy Act

Biometrics

Technology not the driving issue

We've figured it out (mostly)

- UCORE, NIEM, MIEM and TWPDES

NIEM
BRIDGING INFORMATION SYSTEMS

Challenges with US Visit

- Segmentation issue
  - Criminal information in IAFIS
  - Criminal and Civil Information in IDENT
- MOUs with others
  - Impacting FBI and FBI customers without realizing the potential damage
  - Not following Guideline 4
- Without Exit – pushing more work on FBI systems
- Keeping data up to date, especially expunged records – (2 systems vs. 1 system)
  - Audits are slow and expensive

Concluding Thoughts

- Can't separate biometrics from other sharing efforts
- Can't fund biometrics separately
- Standards are good….and needed
- It's a complex issue that requires policy makers to pay attention as it touches:
  - Access
  - Privacy
  - Safety of the Homeland

NIEM
BRIDGING INFORMATION SYSTEMS

Homeland Security Presidential Directive – 24 (HSPD-24)

June 5, 2008

NDIA
National Defense Industrial Association

A forcing function: HSPD 24 will require data sharing

POLICY

PRIVACY

STANDARDS

LEGAL

POLITICAL

TECHNOLOGY

INDUSTRY

HSPD 24: "Many agencies already collect biographic and biometric information in their identification and screening processes."

HSPD-24 Key Issues

Policy…"…make available to other agencies all biometric and associated biographic and contextual information associated with persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security." (Para 11)

Technology…"Recommended executive branch biometric standards are contained in the Registry of the United States Government…updated by NSTC Subcommittee on biometrics and Identity Management." (Para 18)

HSPD-24 Key Issues

Attorney General…

- With the Secretaries of State, Defense and Homeland Security, the DNI and the Director of the Office of Science and Technology Policy...submit to the President an action plan to implement HSPD-24. (Para 19)

  - Recommend categories of individuals in addition to KST (Know and Suspected Terrorists) who may pose a threat to national security threat.

Draft DoJ Action Plan October 08

Eight (8) Primary Biometric Databases:

1. FBI Integrated Automatic Fingerprint ID System (IAFIS)
2. National DNA Index System (NDIS)
3. DoD Automated Biometric Identification System (ABIS)
4. DNA Intelligence DNA Database

Draft DoJ Action Plan October 08

Eight (8) Primary Biometric Databases:

5. DHS Automated Biometric Identification System (IDENT)
6. DOS Facial Recognition System (DOS FR System)
7. Terrorist Identities Datamart Environment (TIDE)
8. Terrorist Screening Database (TSDB)

Draft DoJ Action Plan October 08

National Security Threats (NST)…New category in addition to KST who may pose a national security threat; these categories is not intended to be an exhaustive list of person who may pose a threat to national security

NST Centralized and decentralized options…

- Decentralized would require agencies that identify NST to make info available to other agencies.
- Centralized is similar to KST operations.

NDIA
National Defense Industrial Association

Managing Identities across the full spectrum of mission sets

A Biometric Enterprise to Defeat Terrorist Networks and Secure our Borders

NDIA Biometrics Committee

Martha Karlovic

martha.a.karlovic@saic.com

703-349-9405

Tom Giboney

tom.giboney@gmail.com

703-505-0283

NDIA 2009 Biometrics Conference

January 28, 2009

Identity and Access Management for the Extended Enterprise

Paul Grant
Special Assistant for Identity Management and External Partnering
DoD CIO
Paul.Grant@OSD.Mil

Create an Information Advantage for our People and Mission Partners

Value Proposition is The Context

- **Strong IdAM are Key to Info Sharing in Cyber Space and in Physical Access to Sensitive Locations**
  - **Identity Management**
    - **Who are you?**
    - **DoD Accepting eAuthentication Level 4 (aka FBCA Med-HW and Above)**
  - **Access Management**
    - **Enforcement of Sharing Policies**
    - **Based up Resource Attributes**
- **Exploit Investments in Capabilities, Standards, Policies/Rules**
    - **Three Classification Fabrics**
    - **Extended Enterprise (ISE) (Particularly 24/7 Partners)**
    - **Unanticipated & Less Mature Mission Partners**

Where Are We Today

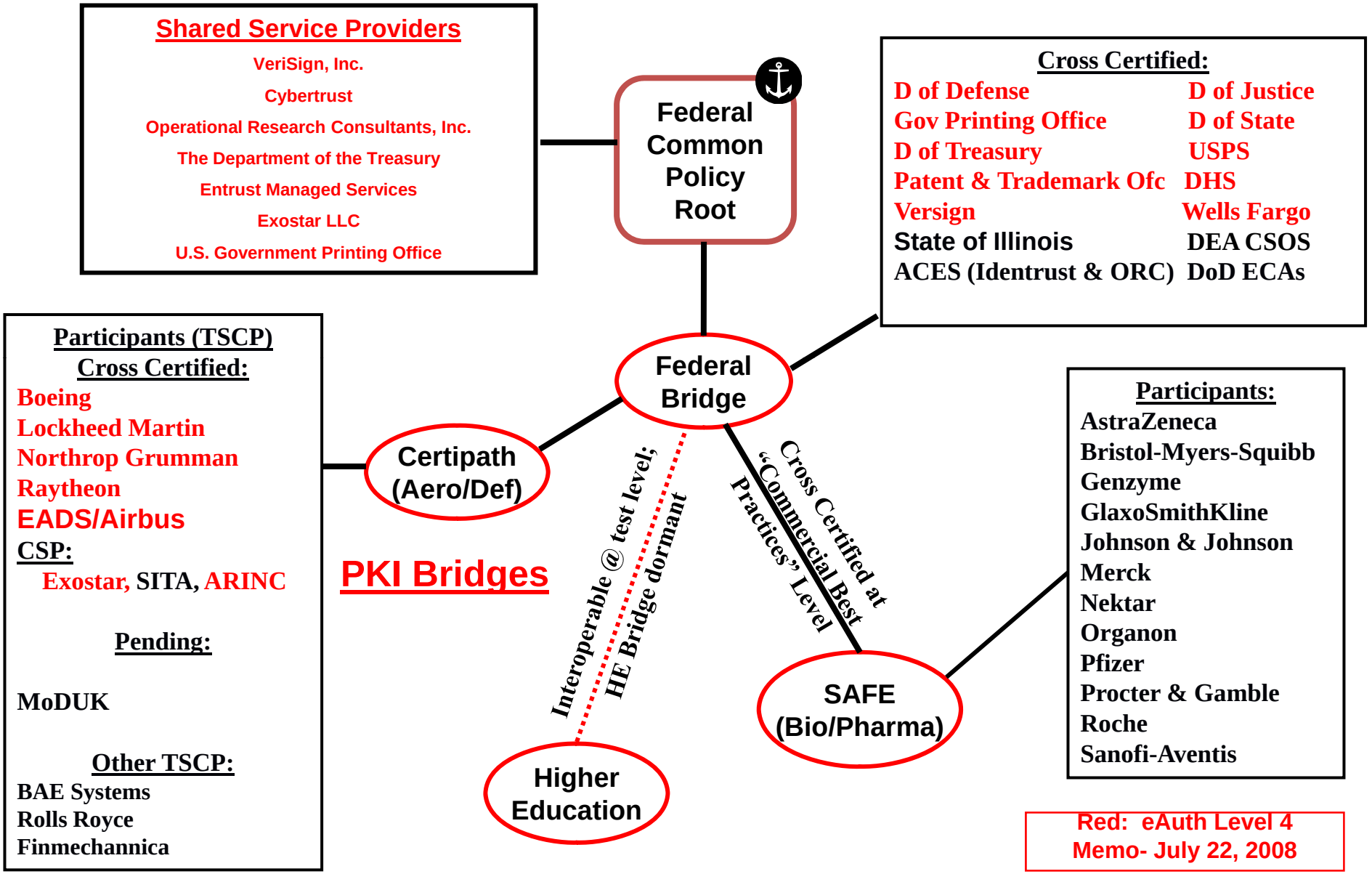
- **Major Identity Management Thrusts:**
  - **Federal Identity Credentialing Committee, FPKIPA**
  - **DoD-DNI Joint Efforts on the Classified Fabrics**
  - **CNSS for National Security Systems**
- **Major Access Management Thrusts:**
  - **Federal Backend Attribute Exchange (derivative of HSPD-12)**
  - **DoD-DNI Joint Efforts on the Classified Fabrics**
  - **IC/DoD Authorization & Attribute Services Tiger Team**
    - **Advancing ABAC/ICABAAD**
- **DoD is Member of the Federal IdAM Federation**
- **External Partners are Following Our Lead With Their Investments**

Expansion of DoD Approved External PKI Memo of July 22, 2008

The following PKIs are approved for use with DoD information systems upon successful completion of interoperability testing.

- **FBCA member PKIs cross certified at Medium Hardware or High Assurance Levels**
- **PKI members of other PKI Bridges that are cross certified at FBCA Medium Hardware or High Assurance Levels**
- **PKIs that Assert the Federal PKI Common Policy Medium Hardware or High Assurance Levels**
- **Also, Approved Foreign, Allied, Coalition partner and other External PKIs (described in attachment to memo)**

Identity Federations



Jasnuary 2009

Fed Bridge Status: http://www.cio.gov/fpkia/crosscert.htm

PIV Fielding Status: http://www.idmanagement.gov/drilldown.cfm?action=agency_hspd12_impl_rpt

Interoperability Testing of Approved External PKI Memo July 22, 2008

- **Purpose**
  - **Ensure that certificates are technically interoperable with DoD systems, and certificate revocation information can be obtained by DoD systems**
- **Content**
  - **Tests interoperability using Direct Trust method**
  - **Tests interoperability using Cross-Certification method**
  - **Use cases: Client Authentication to a Generic Web Site**
    Digital Signing and/or Encrypting Email
- **Status**
  - **DISA is scheduling qualified* Certipath member PKIs for JITC testing began at the end of September 2008**
  - **Developing Interoperating MOA for non-Federal external PKIs**
    - **Internal DoD legal requirement**
    - **Covers Responsibilities, Termination of interoperating, Liabilities, etc.**

***PKIs from other PKI Bridges, cross certified with the FBCA at the Medium Hardware level of Assurance**

JITC Interoperability Testing

- **Test Plan – Developed in testing between JITC and DoS**

  http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html

- **Federal Partner Test Schedule**
  - **Complete – State, Treasury, Justice, Transportation, EPA, NOAA,**
  - **Discussions started with Others**

- **Other Bridge Testing (Certipath)**

Enterprise	Sponsor	Test Start Date
Boeing	Army FCS	Complete
Lockheed	Army FCS	Complete
Northrop G	Navy SUPSHIP	Complete
Raytheon	Army FCS	Complete
UAL (Exostar)	USAF Exec Fleet	TBD

Recent and Emerging Successes

- DoD Approved External PKI List Extended
- Joint Lessons Learned Information System
- Future Combat System Collaboration
- Security Cooperation Information Portal (Foreign Military Sales)
- Synchronized Predeployment and Operational Tracker (SPOT)
- Defense Industrial Base Critical Infrastructure Protection

Partner Expectations

Partners Can Expect

- Strong Credentialing of our Employees (Authentication)
- Access to Our Public Key Encryption Certificates
- Access to Robust Certificate Status Service
- Service Access to Attribute Service (Authorization) – Future

Expectations from Partners

- The Same as From Us for 24/7 Partners – Plus
- Binding Federation Governance Agreement(s) / Rules that Establish and Maintain Trust
- Consistency on Unanticipated & Less Mature Partners

Summary

Strong Identity and Access Management Are Key to Information Sharing and Collaboration

- **We Need a Clear, Concise, Consistent, Published Course for Ourselves and Our Mission Partners.**
- **Mission Partners are Fielding Strong Identity & Managed Credentials (PKI) as well as Identity Federations**
- **Progress Continues in IdAM Expansion toward Consistent Dynamic Policy-Based Sharing**

DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER

Backup

Credential Service Providers (at eAuth-4) for External Partners (non-Federal)

- **CSPs on Fed Bridge at eAuth-4**

  http://www.cio.gov/fpkia/crosscert.htm

  - **Verisign**
  - **Wells Fargo**

- **CSPs on Other Bridges at eAuth-4 (Certipath only today)**

  http://www.certipath.com/pki-ts.htm

  - **Exostar**
  - **ARINC**

Status, Fabric by Fabric

- **TS/SCI Fabric**
  - **Environment: Homogeneous**
  - **Lead is DNI/CIO**
  - **PKI: IC PKI available for authentication by US**
  - **Federation: Among IC Certificate Authorities (CAs) and Commonwealth CAs**
  - **Notes: Enterprise services for central identity management, Enterprise attribute, authentication, and authorization services**

- **Secret Fabric**
  - **Environment: More diverse**
  - **Lead: CNSS (DoD CIO Chairs)**
  - **PKI: Minimal, CNSS PKI WG Recommendations for SAB. DoD implementing in FY09**
  - **Federation: Commensurate with CNSS Authority (DoD CIO Chairs)**
  - **Notes: No centralized Identity Mgmt, Therefore immature IdAM environment at this time**

- **Unclassified Fabric**
  - **Environment: Extremely Diverse, Complex Environment**
  - **Lead: No Single Lead; Must Cooperate & Federate (DoD & Exec Branch are Heavies)**
  - **PKI: 24/7 Partners Adopting eAuthentication Level 4**
  - **Federation: Federal Identity & Access Management Federation is Central**
  - **Notes: Multiple enclave-specific IdAM services, Most Partners Not Yet Mature**

Key Conceptual Threads
in DoD Net-Centric Information Sharing

- **Extended Enterprise**
  - All Internal and External Participants Required for Mission Success
  - Facilitates Collaborative and Coordinated Decision Making
  - Shared Situational Awareness and Improved Knowledge
- **Federation**
  - Autonomous Organizations Operating Under a Common Rule Set for a Common Purpose
  - Legally Binding Framework Policies, Standards and Protections to Establish and Maintain Trust
- **Information Mobility**
  - Dynamic Availability of Information.
  - Enhanced or Impeded by Culture, Policy, Governance, Economics and Resources and Technology and Infrastructure
- **Trust / Trustworthiness**
  - Cornerstone of Information Sharing is Trust in Partner Enterprises
  - Trusting Policies, Procedures, Systems, Networks, and Data

Threads permeate all Information Sharing Activities

IdAM Collaboration

- **DoD / IC**
  - **DoD/IC PKI Tiger Team**
    - **Coordinate and align on hardware authentication solution**
    - **Develop comprehensive PKI solution for our mission partners**
  - **DoD/IC Authorization and Attribute Services Tiger Team (AATT)**
    - **Co-Chairs: NSA and DOD/CIO**
    - **Advance Dynamic Policy-Based Sharing Capabilities**
  - **Cover Tiger Team**
    - **Provide recommendations on the use and protection of identities**
- **Federal (Created by OMB and Federal CIO Council)**
  - **Federal Identity Credentialing Committee**
  - **Federal PKI Policy Authority**
  - **HSPD-12 Executive Steering Committee**
  - **eAuthentication Executive Steering Committee**

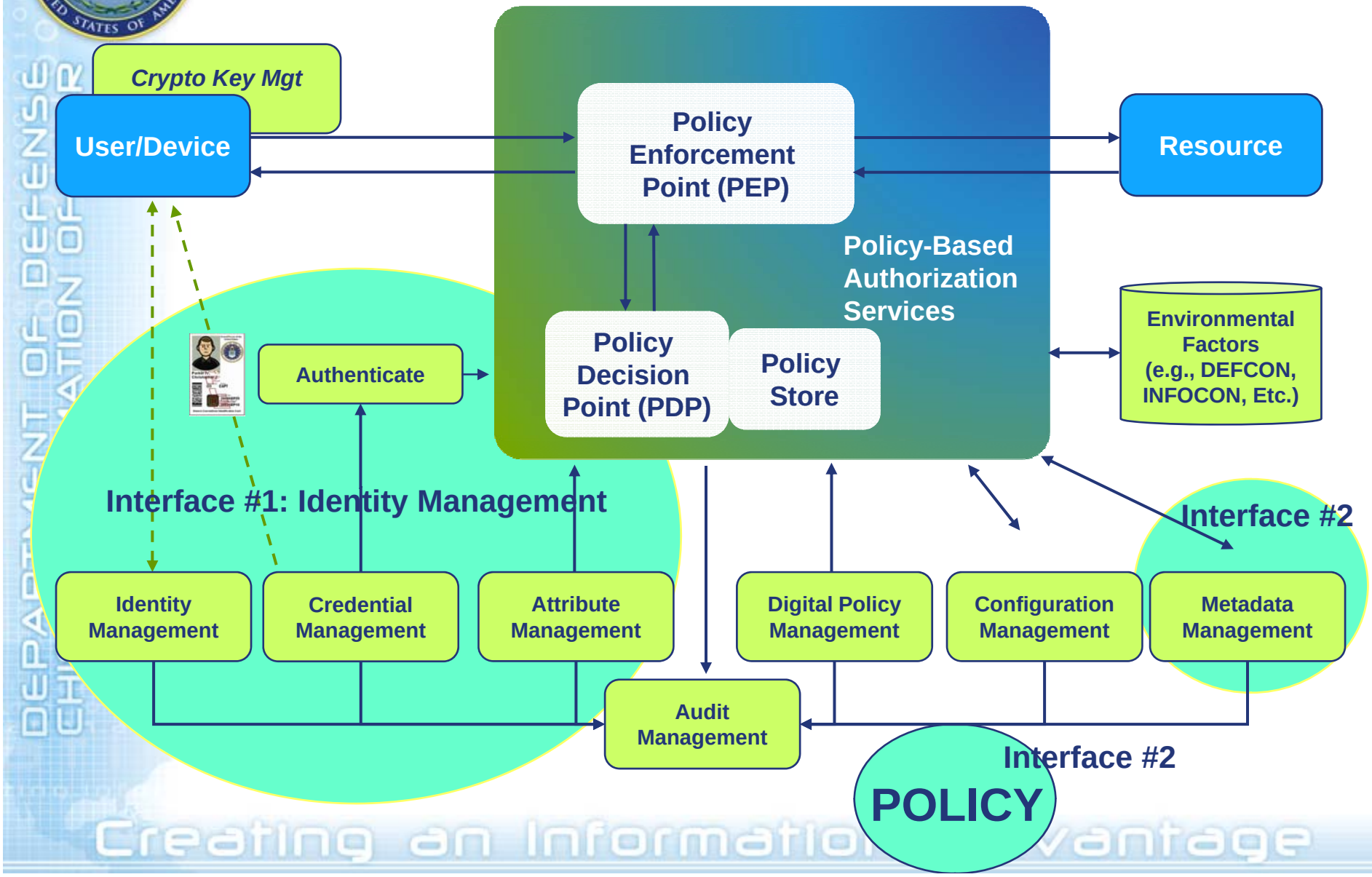
Identity and Access Management
Unclassified Sharing

- **Internally**
  - Operations - Mission & Business
    - Strong Id Proofing & Vetting (eAuth Level-4 & CAC/PIV)
    - Static ACL and limited ABAC (internally)
  - Non-CAC/PIV Holders (e.g., Family Accounts)
    - eAuth Level 2 or Level 3 Credentials
    - Limited functionality – Bounded privileges

- **External Partners**
  - 24/7 Partners - eAuth Level 4 and static ACL
  - Unanticipated & Less Mature Partners
    - Situational Dependency
    - Under Development for controlled functionality / privileges

- **Partner Expectations**
  - Strong Credentialing of Employees (Authentication)
  - Access to Public Key Encryption Certificates
  - Access to Robust Certificate Status Service
  - Service Access to Attribute Service (Authorization) – Future
  - Binding Federation Governance Agreement(s) / Rules(s) that Establish and Maintain Trust
  - Consistency on Unanticipated & Less Mature Partners

Dynamic Attribute-Based Access Management is Policy Compliant Information Sharing




UNITED STATES
NORTHERN COMMAND

Overview

- **Mission**
- **Area of Responsibility**
- **Operations**
- **Interagency Collaboration**
- **Initiatives supported by HSPD-24**

UNCLASSIFIED

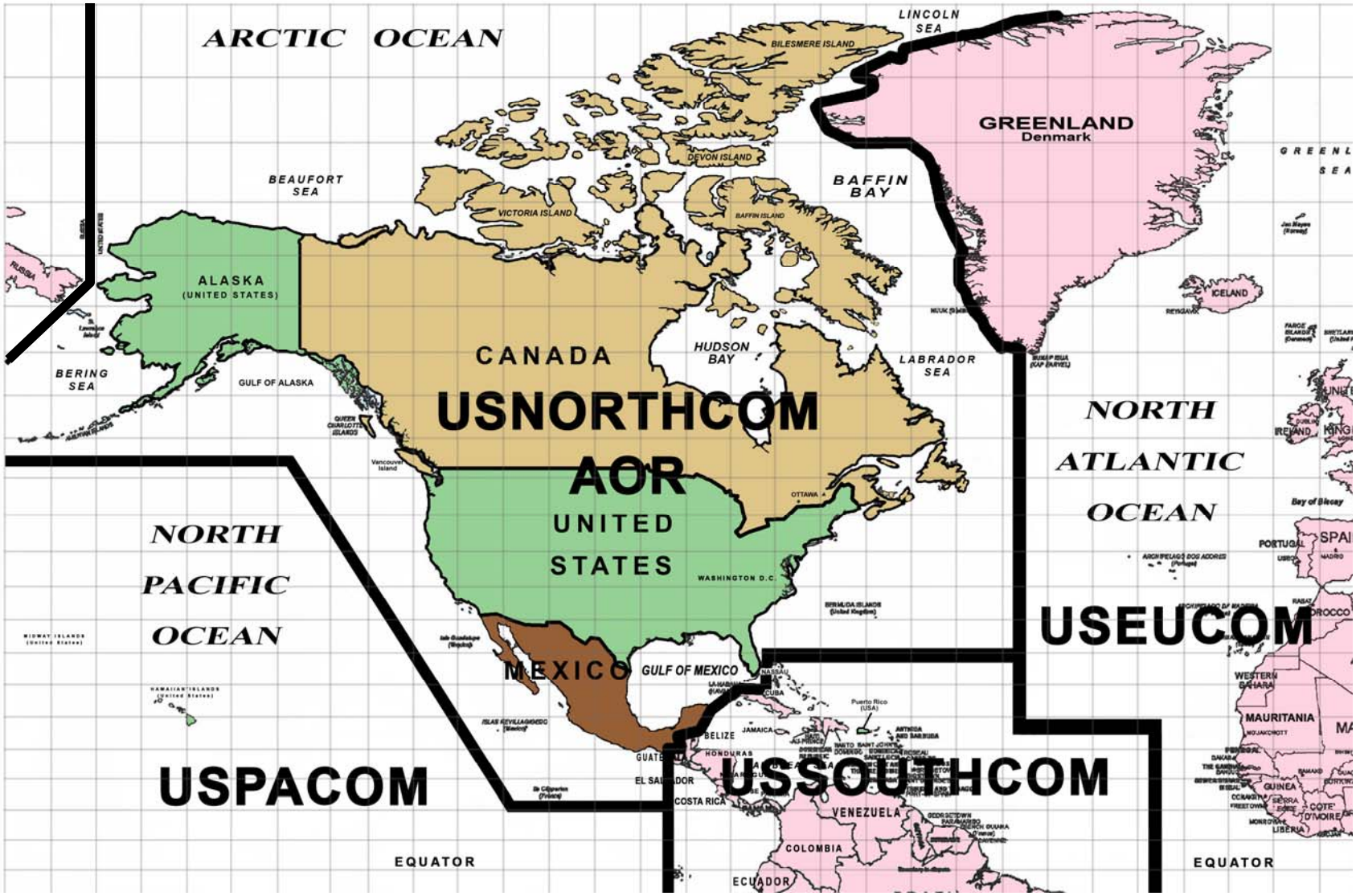
USNORTHCOM Mission

USNORTHCOM MISSION STATEMENT

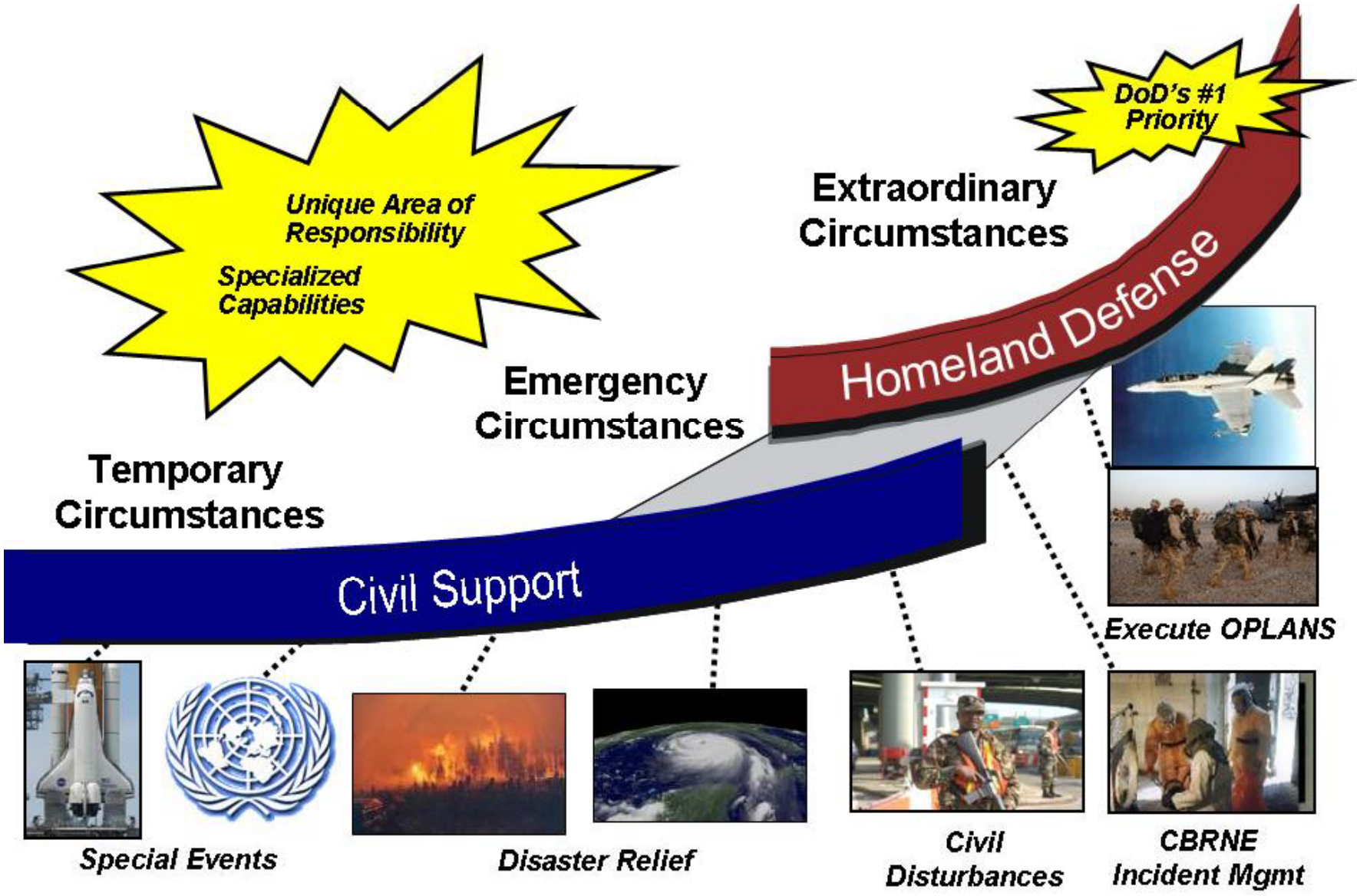
USNORTHCOM anticipates and conducts Homeland Defense and Civil Support operations within the assigned area of responsibility to defend, protect, and secure the United States and its interests.

USNORTHCOM defends America's homeland—protecting our people, national power, and freedom of action

Area of Responsibility



Protecting the Homeland



Interagency Cooperation and Collaboration

Canada Command

Public Safety and Emergency Management Canada

American Red Cross

Transport Canada

Over 60 Organizations are part of our Team

Redefining Jointness…Success Through Effective Relationships

Initiatives Supported by HSPD-24

- **Biometrically-Enabled Access Control at all DOD installations**
  - **Enterprise database with common alerts**
  - **Vetting using shared Federal databases**
- **Maritime Interdiction; cooperation with the US Naval Criminal Investigative Services (NCIS) and USCG; improved handheld devices connected to common databases**
- **Protection of borders**
- **Collaboration with all mission partners to share common data**


USNORTHCOM
Defending our
Homeland

“Strategies For Implementing HSPD - 24”

HSPD -24 From a State and Local Perspective

Kenneth F. Martin
Past President, IAI
Tel. 508-277-5037
E-Mail: kenneth.martin@pol.state.ma.us

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Purpose
  - This directive establishes a framework to ensure that Federal executive departments and agencies (agencies) use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Scope
  - (5) This directive does not impose requirements on State, local, or tribal authorities or on the private sector. It does not provide new authority to agencies for collection, retention, or dissemination of information or for identification and screening activities.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Definitions
  - (a) "Biometrics" refers to the measurable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition; examples include fingerprint, face, and iris recognition; and
    - (NGI- Next Generation Identification: Scars, Marks, and Tattoos)
  - (b) "Interoperability" refers to the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Policy
  - (11) Through integrated processes and interoperable systems, agencies shall, to the fullest extent permitted by law, make available to other agencies all biometric and associated biographic and contextual information associated with persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Policy
  - (12) All agencies shall execute this directive in a lawful and appropriate manner, respecting the information privacy and other legal rights of individuals under United States law, maintaining data integrity and security, and protecting intelligence sources, methods, activities, and sensitive law enforcement information.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Roles and Responsibilities
  - (14) Agencies shall undertake the roles and responsibilities herein to the fullest extent permitted by law, consistent with the policy of this directive, including appropriate safeguards for information privacy and other legal rights, and in consultation with State, local, and tribal authorities, where appropriate.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Roles and Responsibilities
  - (16) Each of the Secretaries of State, Defense, and Homeland Security, the Attorney General, the DNI, and the heads of other appropriate agencies, shall:
    - (a) Develop and implement mutually compatible guidelines for each respective agency for the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information, to the fullest extent practicable, lawful, and necessary to protect national security;

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Roles and Responsibilities
  - (16) Each of the Secretaries of State, Defense, and Homeland Security, the Attorney General, the DNI, and the heads of other appropriate agencies, shall:
    - b) Maintain and enhance interoperability among agency biometric and associated biographic systems, by utilizing common information technology and data standards, protocols, and interfaces;

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Roles and Responsibilities
  - (16) Each of the Secretaries of State, Defense, and Homeland Security, the Attorney General, the DNI, and the heads of other appropriate agencies, shall:
    - (e) Program for and budget sufficient resources to support the development, operation, maintenance, and upgrade of biometric capabilities consistent with this directive and with such instructions as the Director of the Office of Management and Budget may provide; and

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Roles and Responsibilities
  - (18) The Director of the Office of Science and Technology Policy, through the National Science and Technology Council (NSTC), shall coordinate executive branch biometric science and technology policy, including biometric standards and necessary research, development, and conformance testing programs. Recommended executive branch biometric standards
    are contained in the Registry of United States Government

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- NTSC (National Science and Technology Council)
  - The National Science and Technology Council (NSTC) was established by Executive Order on November 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise. Chaired by the President, the membership of the NSTC is made up of the Vice President, the Director of the Office of Science and Technology Policy, Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- NIST (National Institute of Standards and Technology)
  - Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- 9/11 COMMISSION ACT OF 2007 PUBLIC LAW 110–53—AUG. 3, 2007
  - This law is all-encompassing, and is 286 pages long
  - Law Enforcement Terrorism Prevention Program
  - The Department of Homeland Security (DHS) will establish an Office of State and Local Law Enforcement to serve as a liaison to state, local and tribal (SLT) law enforcement on policy issues
  - DHS will provide support to fusion centers
  - Sharing of information

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Local Law Consideration
  - Obtained at time of arrest vs. conviction retention
    - Fingerprint
      - Inked record vs. Electronic enrollment
    - DNA
      - Crime categories allowing collection
      - Time of arrest vs. conviction vs. condition of release
  - Allowable collections by law
    - Fingerprint Law – Massachusetts “felony or by virtue of process”
    - Medical Examiners Offices – overworked / understaffed / underfunded
  - Wiretap Laws
    - 1 party = 33 states
    - 2 party = 16 states
    - Federal Law = 2
  - Juveniles

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- AFIS – Automated Fingerprint Identification System
  - Unlike CODIS or NIBIN, AFIS is decentralized
    - Combined DNA Index System
    - National Integrated Ballistics Information Network
  - 100's of systems currently in use
  - Perceived philosophy
    - Enter Once
    - Search Many

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- AFIS – Automated Fingerprint Identification System
  - AFIS – almost 30 years
  - IAI Conference predicted interoperability by 1995
    - Currently still no interoperability
      - Big Four
    - Can't even get a directory of users
- IAFIS – Integrated Automated Fingerprint Identification System
  - Federal System
  - July 1999 Operational
  - Approximately 56 million records (voluntary system)
- NGI – Next Generation Identification
  - Palmprints
  - Scars, Marks, and Tattoos

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Standards to be interoperable and the technology to be widely connected have existed for at least a decade
- To the contrary, the capability to search is quite limited and does not provide all the potential that should be exploited for such a powerful tool in our arsenal to fight crime, identify terrorists, and even potentially prevent acts of terrorism

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Law enforcement managers seem reluctant to permit the open connectivity without understanding the consequences, and rightly so
  - MOU's
- Connectivity/networking/interoperability inadequacies
  - States can't search state to state
    - Some cases within their own state
  - Nor can federal law enforcement search directly against a certain state's files
- All fingerprint records are not centrally located
  - Many reasons why
  - Mobility of criminals

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Address the need to maintain accuracy of records
  - Image quality issues
- Workload management
  - 24/7 Units
  - Resources
    - Hardware Costs
    - Personnel Costs
- Provide up-to-date information for what each agency can support
  - How many searches will be allowed
- Authentication of record card
  - MOU or Federal Law may be necessary

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Information Sharing
  - Most information currently coming down is criminal in nature
  - “Right to know vs. need to know”
  - Most information over classified
    - Sensitive law enforcement information
  - Many states have laws concerning information release
    - Reasons allowed
    - What type of information allowed
    - To whom the information may be released to
      - Once out of state surrendering state has no control
    - Penalties may be associated

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

- Recipe for Success
  - Adequate resources committed to this endeavor
    - Personnel
    - Hardware
  - National legislation/ MOU
    - Standardization
      - SOP's concerning collection and dissemination
  - Resolve connectivity / networking / interoperability inadequacies

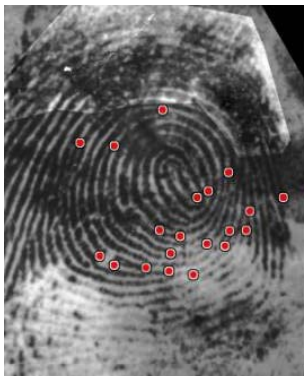
Policy Strategies for Implementing HSPD-24

Al Miller

January 27, 2009

Biometrics: Discovery of New Ways to Protect the Homeland

BIOMETRICS TASK FORCE



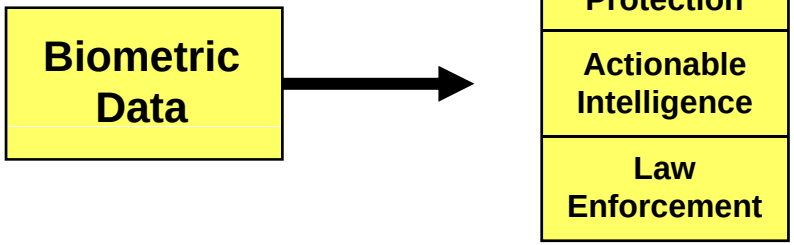
Name:

[redacted]

Date of Birth:
20 October 1980

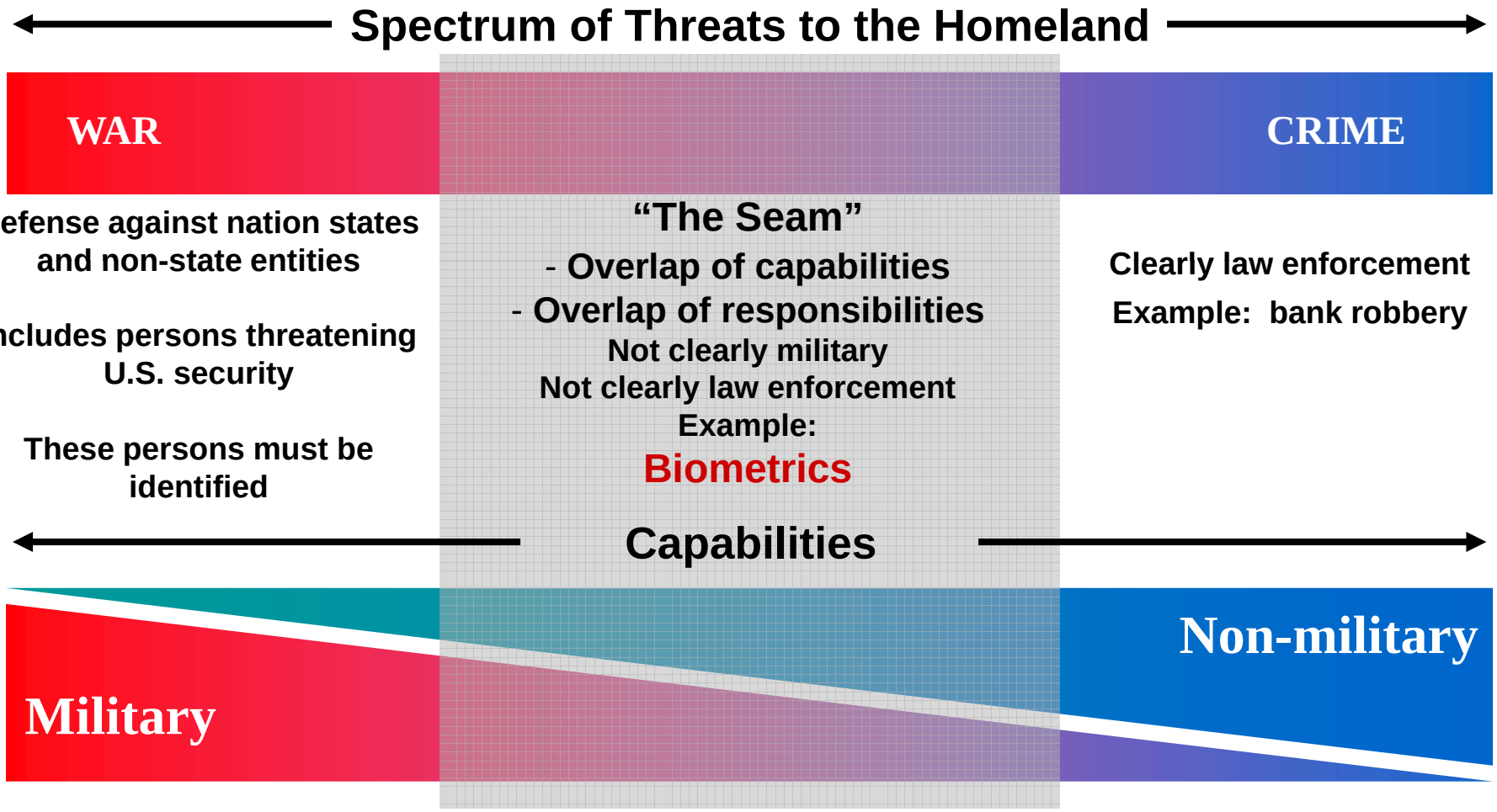
Place of Birth:
Iraq

- Late 2004 - Iraq detainee fingerprinted with data sent to DoD Biometric Fusion Center (BFC)
- Jan 2005 - Terrorist Explosives Device Analytical Center (TEDAC) provided latent fingerprints recovered from an Improvised Explosive Device (IED) to BFC
  - BFC manually processed latent prints for use in DoD Automated Biometric Identification System (ABIS)
- Jan 18, 2005, BFC matched detainee's prints to latent images found on IED; the FBI Laboratory confirmed match
  - BMO/BFC coordinated identification of detainee with FBI, Army G-2, the National Ground Intelligence Center (NGIC), the National Detainee Reporting Center (NDRC), and CENTCOM
- Today - Suspect being detained by CENTCOM Force Protection Forces pending further investigation



Spectrum of Policies: Military or Civilian? Biometrics is a Nexus

BIOMETRICS TASK FORCE



Transition of the Nation's Biometric Activities from Discovery to Policy

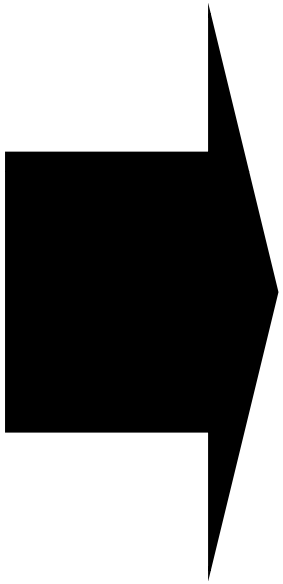
BIOMETRICS TASK FORCE

Homeland Security Presidential Directive HSPD-6
"Integration and Use of Screening Information"

Homeland Security Presidential Directive HSPD-11
"Comprehensive Terrorist-Related Screening Procedures"

Homeland Security Presidential Directive HSPD-12
"Policy for a Common Identification Standard for Federal Employees and Contractors"

National Security Presidential Directive - 59
Homeland Security Presidential Directive - 24
"Biometrics for Identification and Screening to Enhance National Security"



National Science and Technology Council Subcommittee on Biometrics and Identity Management

(IdM Task Force)

Way Ahead

BIOMETRICS TASK FORCE

- Integrate identity management techniques, including Biometrics, in civil, commercial and academic activities
- Leverage biometrics as an enabler of cooperation
- Encourage Private Sector Partnerships to enhance future federal interagency identity management efforts
- Strengthen Global Partnerships through interoperability and information sharing

HSPD-24
Policy Panel Discussion

Robert A. Mocny, US-VISIT Director

Homeland Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

Biometrics Revolutionize Security

BEFORE US-VISIT	SINCE US-VISIT
Paper-based travel documents were susceptible to fraud, alteration	Significantly increased ability to detect fraudulent /altered travel document use
Officials relied on biographic information, which can be forged, to verify identity and make visa issuance or admission decisions	Officials use biometrics, which are virtually impossible to forge, to prevent dangerous people from obtaining visas or entering the United States
Disparate information systems lacked coordination	Better coordination with other agencies; provide a single source for biometrics-based information on dangerous people
Countries operated independently from one another on law and immigration enforcement	Countries are adopting similar standards to stop criminals, immigration violators and known or suspected terrorists

Homeland Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

Users of US-VISIT's Biometric Identification and Analysis Services

Homeland Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

Upgrade to 10-Fingerprint Collection and DHS/FBI Interoperability

- **Makes biometric identification and verification process more accurate and efficient.**
- **Consistent with international standards.**
- **Improves latent fingerprint matching.**
- **Technology acquisition and development process required significant interagency collaboration.**
- **Improves interoperability between DHS and FBI biometric systems.**

Homeland Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

New Technologies and Standards: Multimodal Biometrics

- Multimodal biometrics are the next generation of secure identity management.
- US-VISIT is partnering with other agencies to conduct simulated tests on face and iris biometric technology to evaluate the current market and its state of maturity.

Homeland Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

New Technologies and Standards: Mobile Biometrics

- Demand for mobile biometric technology is increasing.
- US-VISIT has successfully tested the capability to check biometrics from a remote location through a wireless, mobile solution.
- DHS is examining broader application of mobile biometric technology.

Homeland Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

US-VISIT: Committed to Protecting Privacy

US-VISIT fosters a culture that values protecting information

Privacy Protections

- Privacy Officer.
- Carefully monitored systems and security practices in place.
- Partners must adhere to US-VISIT's privacy and security procedures; including privacy training

Transparency

- Extend to non-U.S. citizens many of the same protections that are guaranteed by law to U.S. citizens.
- Privacy impact assessments and system of records notices provide a transparent view of what information we collect, why we collect it, how it is used and how it is protected.

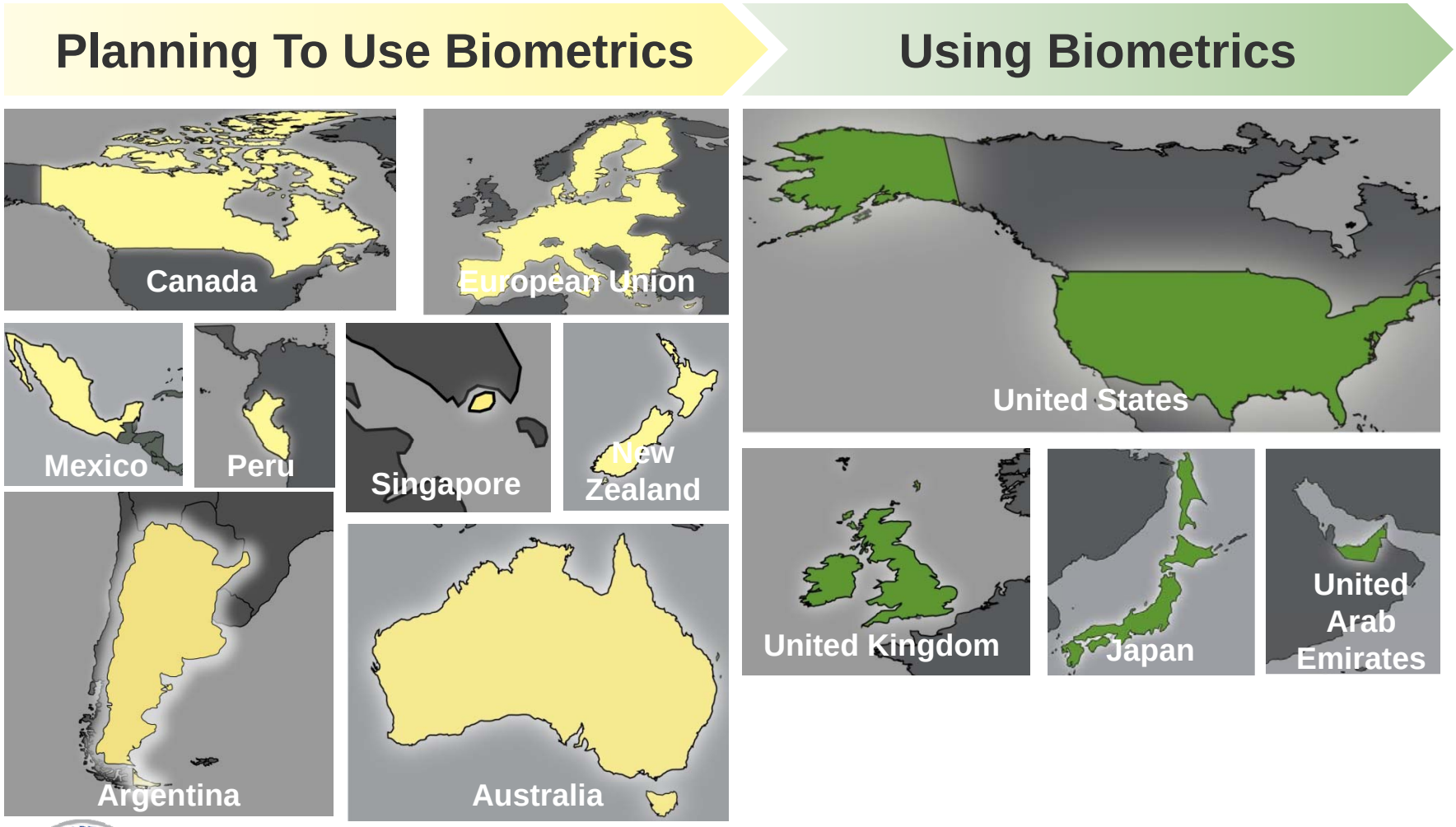
Redress

- Offer visitors resolution through Traveler Redress Inquiry Program (DHS TRIP).

Challenges Ahead for HSPD-24

- Interagency collaboration to advance technology.
- Developing common standards for new technologies.
- Agreement and adherence to strict privacy policies.

Growing Global Use of Biometrics

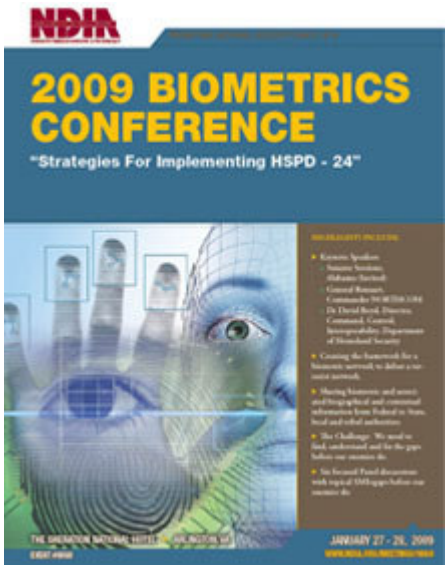


Homeland Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

National Defense Industrial Association

2009 BIOMETRICS CONFERENCE "STRATEGIES FOR IMPLEMENTING HSPD-24" MEETING MINUTES



Location: Washington, D.C.
Date: 27 & 28 January 2009

Table of Contents

Introduction and Purpose

This document contains detailed notes on selected speaker presentations and panel discussions from the 2009 NDIA Biometrics Conference – "Strategies for Implementing HSPD-24". This document serves as meeting minutes from the conference, it is based on notes taken during the conference, and is not a comprehensive account of every presentation or discussion. The "*Q&A Session*s" are not included in every section, only select questions and answers appear in certain sections, and the lists are not exhaustive. All presentations from this conference are available at the NDIA website.

The author of this document is Mr. Benji Hutchinson. Please forward comments or questions to **james.hutchinson@hqda.army.mil** or call 703-607-1951. Mr. Hutchinson is an Associate at Booz Allen Hamilton. He has 5 years experience supporting large-scale biometrics programs at the Department of Defense (DoD) and the Department of State (DoS). He currently supports the US Army Biometrics Task Force (BTF). Mr. Hutchinson holds an M.A. in International Relations and an M.A in French from the University of Kentucky.

1. Day One

Opening Remarks

From the NDIA Committee on Biometrics, Ms. Martha Karlovic and Mr. Thomas Giboney kicked off the conference by providing a summary of Homeland Security Presidential Directive (HSPD) 24 and an overview of upcoming conference discussions on strategies to effectively implement the goals of the presidential directive.

HSPD 24 is a forcing function – it will require data sharing. Many agencies already collect biometric, biographic, and contextual information in their identification and screening processes. HSPD-24 is about policy, privacy, legal, standards, political, technology and industry initiatives. HSPD-24 directs agencies "to make available to other agencies all biometric and associated biographic and contextual information associated with persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security." To effectively achieve the goal of data sharing, HSPD-24 offers recommended biometric standards contained in the *Registry of United States Government (USG) Recommended Biometric Standards*, which is maintained by the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management (IdM). The goal of sharing this biometric data is to further develop and enhance the USG capability to screen for individuals that pose a threat to national security. Two specific categories named and implied are Known and Suspected Terrorists (KST) and National Security Threats (NST), respectively.

An important action item within HSPD-24 calls for the Attorney General, with the Secretaries of State, Defense and Homeland Security, the Director of National Intelligence (DNI) and the Director of the Office of Science and Technology Policy, to submit to the President an action plan to implement HSPD-24. Two general philosophies exist on how to build such a large-scale biometrics screening capability: centralized and decentralized. A decentralized option would require agencies that identify NST to make info available to other agencies. A centralized option is similar to KST operations. Regardless of the solution, the mission is to manage identities across the full spectrum of mission sets and to develop a biometric enterprise to defeat terrorist networks and secure our borders.

The primary challenges facing the United States (US) biometrics community include interoperability gaps, adherence to biometric standards, lack of clear government policy, and privacy concerns.

Keynote Speakers

Key Issues

- Interoperability & Standards
- Policy
- Consolidation of Congressional Oversight and Funding

A. Honorable Senator Jeff Sessions of Alabama

Senator Sessions began his remarks by reflecting on the events of September 11, 2001 and underscoring the importance of identifying dangerous individuals by using biometrics technology for screening. Biometrics as a tool strips the cloak of secrecy from threatening individuals, stressed the Senator, and denies terrorists of their anonymity. Biometrics technology is a critical enabler against terror and crime and it is an essential identification technology. The Senator highlighted major advancements in the field of biometrics. He highlighted the implementation of the automated identification systems, such as the capability maintained by the FBI.

The Senator expanded upon the goal of HSPD-24, which is to facilitate enterprise wide USG sharing of biometrics, biographic, and contextual data, to effectively screen for certain categories of threats. HSPD-24 moves us forward to a network-of-networks and will hopefully force agencies to improve existing identification systems. A long term goal is to achieve an enterprise-wide network-of-networks from the federal level to local police. Reaching these goals will increase mission effectiveness through rapid sharing of identification services, which leads to reduced crime and enhanced national security. A layered approach to identification and screening of individuals incorporates federal, state and local authorities.

The benefits to biometrics and identification technology are apparent in deterring illegal immigration and terrorism. Intelligence on various categories of national security threats is the key to success because it deters illegal entry to the US at land borders. This technology encourages people to enter lawfully in an effective way. Identification checks assist border patrol to notify authorities of illegal entries. Further, identification technology and ensuring the data is shared among agencies decreases the chances of another 9/11 by screening for terrorists.

The Senator outlined major challenges facing the USG associated with reaching these goals. Interoperability and policy continue to challenge the USG with regards to sharing data. The Senator stressed the importance of USG agencies purchasing compatible devices that implement consensus-based biometric standards and the need for the USG to continually establish and maintain memorandum of understanding (MOU) between agencies. Another big challenge facing the USG is a lack of consolidation of oversight for funding of IdM and biometrics related programs in Congress. The 9/11 Commission motivated Congress to fund such programs but the Senator warned against complacency.

Public perception is another big challenge facing identification and biometrics technology. IdM in the US is misunderstood, which creates irrational fear. The biometrics and IdM communities need to demonstrate and explain that the technology is not threatening. There is a need to show that identification systems validate good honest people. Examples of lawful use of identification include driver's licenses that prove you can drive a car, allow one to board an airplane, and historically officials were required to have a letter of introduction. The program eVerify is a good example of a modern technology used to verify someone's identity.

Q&A Session
Q: Could you comment on the use of biometrics for identification to vote?
A: In New Mexico, citizens do not want an ID to vote. In Georgia, citizens need a drivers license to vote. Close elections, a difference of 200 votes makes a difference and people want integrity.
Q: What will the focus on Capitol Hill be with regard to biometrics and HSPD-24? HSPD-24 is a directive that the Obama Administration will review.
A: We can show systems protect privacy rights, don't threaten our liberties but increase our national security. Not take for granted new administration will understand this. If se overall network undermined by policy changes, tell me. See PD-24 on right road, can sustain and will be received.
Q: HSPD-24 guides the USG to share information. Jurisdictions are an issue. Do you see consolidation of oversight on the Hill?
A: No. Committees take the lead, everyone is in the act after that either to stop it or alter the plan. This is democracy in America. After 9/11 there was a lot of momentum and we got a better system. We were motivated. Having not been attacked since then may lead to complacency and this would leave us vulnerable in the future if systems do not talk to each other. The USG needs to stay on top of this. President Bush had researched the law and the laws are consistent with legal rights.

B. General Victor E. Renuart, Jr., North American Aerospace Defense Command and US Northern Command (NORTHCOM)

General Renuart began his remarks by describing his responsibility and the mission of NORTHCOM. The NORTHCOM Mission is to support warfighter and efforts for counterterrorism and regional security and to provide force protection to military installations within the continental US to over 1,400 locations. General Renuart focused his remarks on the challenges associated with his mission and how accurate biometric data and databases support his mission.

Not since the Civil War has the military feared for their families lives in the US. Terrorists do not respect borders. Along the southern US border, a significant amount of weapons and cash moves across the US/Mexico border. This traffic fuels drug cartels. Along the northern US border, snow mobiles are used for transportation across the US/Canada border. Threats from a porous border motivate the use of biometrics and IdM technology. The use of technology allows officials to identify illegal entry at land borders and limits criminal mobility. Over 1 million transited US borders in 2007. Collected biometrics at points of entry stopped 4,000 individual who are criminals. General Renuart stressed the importance of HSPD-24. By building a database that allows users to sense a threat and take action, the US can stop illegal entry and illegal movement of drugs, guns, money and WMD.

The current problem facing NORTHCOM is the vulnerability of facilities to attack and complacency. The US military must become smarter at providing security to its bases. Biometric identification is a viable solution to these challenges. This technology will improve security measures by eliminating the possibility of stolen or forged identification, and improve situational awareness by providing a readily accessible record of who is on base.

General Renuart stressed that the threat to US military installations is real. He provided the example of the failed terrorist plot on Fort Dix, where six individuals planned an assault on the base. The group used a family pizza shop as cover to gain access and conduct surveillance on Fort Dix. The plotters acquired maps of military facilities and planned to slaughter scores of military personnel. A Circuit City clerk discovered a DVD of the men at a firing range and reported it to law enforcement entities at which time the plot was uncovered.

The challenges associated with the application of biometrics technology to the NORTHCOM mission are interoperability, the procurement of standards based equipment, and policy gaps governing the collection of various types of biometric data. The General stressed the importance of pushing industry to build equipment to consensus based standards. DoD must also determine how to push for smarter access control within the existing installation infrastructure. These challenges cannot be put off until the POM cycle. The Services, working in coordination with the Biometrics Task Force (BTF), must facilitate interoperability and common data sets. Common sets of biometric data allow decision makers to provide better security at various points of entry.

Policy Panel Discussion

Key Issues

- Interagency Collaboration on Science and Technology (S&T) Initiatives
- Common Standards
- Agreement and Adherence to Strict Privacy Policy
- Consolidation and Dissemination of Watchlists Across USG

A. Mr. Steve Yonkers , Business Policy and Planning, US-VISIT for Mr. Robert Mocny, Director, US-VISIT Program, Department of Homeland Security
Greatest challenges moving forward are interagency collaboration on technology advancement, common standards, and agreement and adherence to strict privacy policy.

B. Mr. Al Miller, OSD - Policy, *US* Department of Defense
Greatest challenges lie in gaps between capabilities and responsibilities of military and law enforcement entities.

C. Mr. Thomas Bush, III, Assistant Director, Criminal Justice Information Services Division
Moving forward, greater emphasis will be placed on international sharing of biometric data, integrating the intelligence community into unclassified processes, and integrating DNA into the existing USG biometrics enterprise architecture.

D. Mr. Tony Edson, Senior Advisor, Consular Affairs, *US* Department of State
Different organizations capture biometrics to support different missions and HSPD-24 further refines and defines roles and responsibilities for government agencies on how to employ biometrics technology.

Government Panel Discussion

Key Issues

- Consistent Adherence to Biometric Standards
- Obtaining Devices that are Faster, Lighter, and Cheaper
- Political Will to Affect Change
- Common Set of Rules for Sharing Biometrics Data Across the Interagency Landscape

A. Mr. Vickers, Special Assistant to the Director of the Biometrics Task Force (BTF)
Mr. Vickers began his brief with the importance of BTF mission and the implementation of biometrics as a force protection technology. The DoD and its mission is out on the pointy end of the spear. DoD components collect biometrics on population sets of the highest risk for terrorist activity. Biometrics intelligence and data are only valuable when the USG and our allies use it. Purpose of biometrics is to deny enemy anonymity.

"Defense in depth" is a strategy to strip anonymity of individuals abroad and increase the number of encounters with individuals. Moving forward, one challenge will be to engage our multinational allies in sharing efforts to screen threats across databases. DoD Challenges include: interoperability and standards, challenge of obtaining a better, faster, stronger biometrics capability, and the will to impact outcomes through organization, technology, and policy.

B. Ms. Angela Miller, Consular Affairs, US Department of State

Ms. Miller provided an overview of the Department of State (DoS) biometrics capability. The strategy of the DoS is "Open Doors and Secure Borders". The DoS biometrics capability includes three major components: name check, fingerprint check, and facial recognition check.

Fingerprinting at post involves clearance checks. 220 posts send fingerprint data to the Consolidated Consular Database (CCD) which forwards to IDENT, which is a US-VISIT database that contains the biometric information of international travelers to the United States who are enrolled through DHS's US-VISIT program, as well as known or suspected terrorists, criminals, immigration violators and others. Namecheck systems are used to vet applicants of passports and visas. Numbers of name checks have gone from 1,000 to 50,000 from 1970 to 2008. Major Namecheck Tasking – more interagency data sharing, international data sharing of lost and stolen passports, and redesigned CLASS for infinite searches.

The Facial Recognition (FR) System works through the CCD to distribute templates to posts for verification. FR uses three pass analysis: vector feature analysis, local feature analysis, and surface texture analysis (STA) "skin". FR process goes from post capture of face image, to FR software enrollment in CCD, search results are displayed, KCC inspects images, and results return to post.

DoS has the largest facial recognition data base in the world with 73 million images in system. The Chief Information Officer (CIO) of DoS is interested in initiating an iris database. DoS is interested in working closely with BTF to leverage iris technology implemented in Next Generation Automated Biometric Identification System (ABIS). Data available on the CCD is used by DoS, DHS, FBI, DoC, and DoD.

C. Mr. John Kress, Acting Chief, Force Protection and Mission Assurance Division, USNORTHCOM/J34)

NORTHCOM anticipates and conducts Homeland Defense and Civil Support operations within the assigned area of responsibility to defend, protect, and secure the US and its interests. From NORTHCOM perspective, biometrics is predominately an interagency effort.

As a result of HSPD-24, the following initiatives need to be initiated: Biometrically enabled access control at all DoD installations, maritime interdiction, protection of borders, and collaboration with all mission partners to share common data. In the defense of our homeland, one central focus is installation access security.

D. Ms Johnna Hoban for Ms. Kimberly DelGreco, Section Chief, Biometric Service Section, Federal Bureau of Investigation

Ms. Hoban kicked off her brief with a statement of how USG agencies are using biometrics for their own mission specific goals. Currently, 60 million records reside in IAFIS, with biometric, biographic, and contextual data all indexed by fingerprints. Next Generation IAFIS will expand upon IAFIS capability to include flat fingerprints, palm, and potentially other future modalities.

Ms. Hoban provided an overview of the Center of Excellence and its efforts in S&T, standards, and other biometrics efforts. CJIS HSPD-24 initiatives include working with NCTC on KST collection,

storage, use, and sharing of biometric and biographic data. DoJ is a co-chair, along with the Office of the Director of National Intelligence, for the interagency working group on NST.

E. Ms. Patricia Cogswell, Executive Director, Screening Coordination Office, DHS

Ms. Cogswell initiated her brief with definitions of screening and a few statistics of the DHS capability. DHS processes 1.2 million inbound travelers at ports of entry, 630,000 aliens. DHS screens 1.8 million domestic air travelers and conducts 135,000 biometric checks for visa applications. This is set to increase to 300,000 per day by next year. DHS processes 30,000 immigration benefit applications, including asylum seekers. DHS verifies the employment status of 3.2 million new employees, which includes a photo tool that returns an image of individuals. DHS manages trusted traveler programs and designs and executes background checks for critical infrastructure workers.

Current DHS efforts in biometrics include: Watchlist service, TSC/DHS efforts to identify existing biometrics, and R&D efforts. Currently, there is no standardized way to categorize quality across vendors. In the area of 10 print fingerprint enrollment roll out, so far 2,500 workstations have been implemented around the country and they have collected 6.6 million 10 print submissions. TECS is a text database containing the no-fly lists.

Q&A Session

Q: How does one get their record expunged from a DHS whatchlist?
A: TRIP is a request system that allows DHS to examine records.
Q: What is the order of implementation for NGI?
A: Incremental approach on modalities based on the state of the art technology at that time: 1st is palm print, 2nd face and iris, without exact dates. Dates can be provided later.
Q: General comment: NORTHCOM is prepared to purchase equipment using their own dollars and they run the risk of buying non standard equipment.
A: DoD responded by saying DoD entities need to ask this question in appropriate working groups.
Q: What are large scale government agencies doing to anticipate the 5-8 year picture of the USG biometric capability?
A: DoD should have a much tighter coordination effort with law enforcement. DoS is working towards developing a Center Of Excellent (COE) in September 2009 and implementing iris. DoS will probably not do much with all modalities except leveraging existing technology. FBI will be implementing NGI, supporting intelligence, and working with more partners. DHS wants faster, cheaper, smaller because USG biometrics is moving towards a multimodal environment. DHS wants to tag data to develop a common rule set for sharing data across programs, this will decrease barriers to sharing.
Q: Industry needs to know what big projects to invest in?
A: DOS is looking at iris, to get a biometric center together. There is an RFP for iris. NORTHCOM: Program of Record (POR) is where the military services plan into their budgets, the O&M piece. All COCOMS requirements are recognized. FBI: NGI implementation; need fusion to support intelligence and lead value to see the overall picture. Who is the person at a distance collection. Forums talk to industry to tell them the challenges. DHS: Want faster, cheaper. All going Multimodal. Do quick identification, speed is important. Existing biometrics in background, are they no longer eligible to get access. Tad information in a smarter way. Rule sets make sense with programs. Artificial barriers removed to access information. BTF: Digital requests bounce from database to database. Have enough fidelity, need vision, what do with this person.

Commercial Industry Panel Discussion

Key Issues

- Privacy

A. Ms. Katherine Stokes, Associate General Counsel, Graduate Management Admission Council
Ms. Stokes provided an overview of GMAT, which facilitates the movement of talent around the world. Biometrics provides a technological capability to prevent fraud during the administration of GMAT. Legal challenges with fingerprints exist in the US and the European Union (EU). In the US, no right to privacy codified in US Constitution. There is a patchwork of sector and state laws. In Europe, there is a strong sensitivity to fingerprints. The right of privacy is "fundamental human right" essential to civil society, rule of law, and democracy. The Graduate Management Admission Council (GMAC) is the industry leader in privacy compliance worldwide.

GMAT implements palm vein technology, which enhances GMAT security with 1:N matching on the horizon. This technology is designed to meet EU requirements such as user leaves no trace on device, no surreptitious collection, no image stored, and encrypted. Unique Fujitsu-Pearson VUE algorithms, non reversible and not interoperable with other palm vein systems.

B. Mr. Jason Silbeck, Chief Technology Officer, CLEAR
CLEAR is the largest registered traveler program operating at US airports with over 250,000 members since June 2005. Partnerships are established with airports and airlines, plus major marketing partners. Technical interoperability is achieved with all certified registered traveler service providers. All capital and operating costs are supported by voluntary membership – no cost to taxpayer or airports.

Key Points: Attention to customer service can rapidly speed growth and satisfaction. Interoperability provides flexibility and encourages stakeholders. True security benefits are an important part of the service offering. Registered travel has a history dating back to 2004. Vigilent is a competitor to CLEAR. Currently CLEAR collects 10 prints, 2 iris, 1 photo, and biographic/contextual data. The prints and irises are used for matching but not the face. CLEAR card meets the technical requirements for an identification card in the airport, perhaps the only one you'll need because of these features. Interoperability and open technology standards for fingerprint, iris, facial photo, smart card. CLEAR worked with DHS to develop "RTIC Technical Interoperability Specification" published in 2006, provides guidelines for implementers.

Q&A Session
Q: Without getting into the nitty-gritty details, does CLEAR today or in the future plan to use a standardized fingerprint template to exchange data within your architecture? Or is it a proprietary format with the ability to generate the standard, if needed.
A: CLEAR uses standards.
Q: Does CLEAR currently screen biometric samples against IDENT?
A: No, but it could if it needed to do so.
Q: What is the liability of using biometrics for these commercial applications?
A: For CLEAR, they must meet standards put forth by USG and TSA to obtain insurance against terrorism. For GMAT, they comply to several recognized standards.

2. Day Two

Keynote Speakers

Key Issues

- Coordination and Cooperation Between Local, State, and Federal Entities

A. Dr. David Boyd, Director, Command, Control, Interoperability, US Department of Homeland Security

Initiated discussion about the mission of Command Control and Interoperability (CCI). Continued about the communications challenge on the frontlines. Emergency responders, such as police officers, fire personnel, and emergency medical services (EMS), need to share vital data and voice information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large scale emergencies. History dictates which band certain responders use for communications. Certain bands were available during certain times and often times proprietary systems were fielded, which adds to the challenges.

Why does interoperability fail? Locals have almost all the information, about 99%. Local responders know all the details on the ground plus the own the systems collecting information. Federal agencies need locals' data. State and federal direct structures that feed their needs. State and federal usually offer little or no value added or incentive to locals. So, sovereign locals don't play.

In a practitioner-driven approach, a successful strategy for improving interoperability and information sharing must be based on user needs and driven from the bottom up. The Constitution works this way – think of representation vs. federal representation of agencies. This approach ensures that resources are aligned with users. Locals know that they have most of the biometric information. Federal data bases are often searched last because criminals are often located in the state or an adjacent state in which the crime was committed. The key is to incentivize locals to share data with federal systems – we need them more than they need us.

Funding from the federal level for such systems is not as large a contribution as many think. Typically federal funding accounts for a small percentage of the total funding for communications systems. Plus money from the federal government is often slow to arrive. Current interoperability focus is on point to point information exchange boundaries – focus is on the technical interfaces. This focus allows time to be spent on development of standards to create an open framework to facilitate the exchange of information. There are about 60,000 agencies most of which are have a small number of officers and these agencies raise their own funding for equipment.

Current initiatives include interoperability of systems and managing day-to-day information using the National Information Exchange Model (NIEM). Standards are an important aspect of this interoperability process. Project 25 compliance assessment is another program. Data messaging standards support tagging data elements, that will allow users to strip apart data and know how to process it correctly.

Critical Infrastructure Inspection Management System (CIIMS) allows state of Maryland to reroute aircraft after mission is complete during the return flight so as to make the overall flight more efficient. Saves on fuel cost and maintenance fees that can be transferred to other projects.

Q&A Session
Q: In the biometrics world, local proprietary AFIS systems exist at the local level. How do we reach down to that data?
A: No interoperability issues are technological, they are human elements. Leadership commitment is the first hurdle. HSPD's direct federal agencies to fall in line, not the locals. Standard operating procedures and common training courses facilitate interoperability and must be developed. Governance is a critical piece – how does the consensus agree that who will be in charge and who will pay. Locals are sovereign and don't typically have to play.
Q: Do you see more partnerships between the private and public sectors working together to solve interoperability challenges?
A: Yes, federals work with locals by paying for the consensus building process (meetings, travel, etc.). Federal level should not dictate standards – we must begin at the bottom and work our way up.

B. Pete Marone, President, Consortium of Forensic Science Organizations; Director of the Virginia Crime Lab
From his perspective, interoperability is different depending on the level from which you sit. Locals are typically concerned with interoperability with other locals. Federals are concerned with federal interoperability. Mr. Marone spoke about variations in the production of fingerprint templates between various vendor algorithms. Due to proprietary formats, this poses a challenge to locals. Need to work on better ways to standardize digitization of fingerprint cards.

The DNA data in the NDIS systems resides at the state level. When DNA data is stored in the VA database, it resides in a VA column within NDIS. When VA draws down that DNA data, the total number of VA files decreases. In other words, the federals do not control state databases. Locals and states work better together than the locals, states, and federals do. 95% of hits are local, however, hits in other states are increasing. Local entity can't search the federal database. There is a state coordinator that forwards searches from the state level to the federal level. Once a week, state coordinators forwards files to NDIS/CODIS for searches. This is critical for DoD to consider when developing its integrating DNA into the DoD biometrics architecture.

IAFIS does not work that way. "A camel is a horse made in committee." Need to be conscious of this detrimental. Federal level needs to determine how to deal with local requirements that clash with federal requirements, and state requirements for that matter.

Q&A Session
Q: Local, state, and federal data requirements often differ. The challenge to strike the balance between making a system cumbersome and satisfying everyone requirements within a standard. Are there any effective incentives you can share that bring decision makers to the table to discuss these issues? What are some effective ways you've seen to display added value to a system from the consensus driven process besides simply stressing the interoperability language?
A: Locals are goal oriented. Unfunded mandates do not do it.
Q: Going forward, can we resolve interoperability issues by mandating one single ID as opposed to individual state IDs.
A: Deferred to his technical lead.

Technologies Panel Discussion

Key Issues

- Interagency Interoperability
- Quality of Biometric Sample Data
- Indexing, Tagging, and Tracking Biometric Data

A. Mr. Brad Wing, IT Specialist, National Institute of Standards and Technology (NIST)

Mr. Wing began by discussing the NSTC *Registry of USG Recommended Biometric Standards*, which is referenced in HSPD-24. The "Registry" along with other biometrics standards initiatives are addressed within the Office of Science and Technology Policy (OSTP), NSTC Subcommittee on Biometrics and IdM, Standards and Conformity Assessment Working Group. The NSTC Subcommittee on Biometrics and IdM has working groups on policy, standards, RDT&E, conformance testing programs. The Registry lists recommended biometric standards for USG wide use that are available and adopted within many USG organizations. First and foremost, interoperability success depends on the US broad biometrics community knowing that the Registry exists.

The Registry contains standards for collect, store, exchange, transmission profiles, credentialing profiles, technical interface, conformance testing methodology, and performance testing methodology. There is a difference between conformance and performance testing (may conform but have poor performance). The Registry evolves over time. Standards are evaluated and updated to the Registry.

Biometric standards for voice and DNA are under development and will be added to the Registry. Biometric standards for fingerprint, face and other biometrics have already been added. These standards allow for the transmission of biometric information among law enforcement agencies in extensible markup language (XML) format, which is an alternative to binary. The NIST Information Technology Laboratory (ITL) has completed an XML version of the ANSI/NIST ITL 2-2008 standard, titled Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 2: XML Version. This standard will be expanded to handle additional modalities and is used to transmit information to INTERPOL.

Mr. Wing stressed the importance of testing. Conformance testing output is a function of format data process. Performance testing includes error rates, throughput, and responsiveness under various conditions. Who does the Testing? First Party is the manufacturer, Second Party is the user or purchaser, and Third Party is the independent group (Underwriter's Lab). A Robust Standards and Conformance Assessment infrastructure includes Product developers, Second Party, Lab Accreditation, and Third Party validates Certification Bodies. Tools and Standards for Conformance Tests are another critical element for a robust testing infrastructure. In 2005 BioAPI Standard became an ISO standard. In 2006, NIST's Image Group's Minutiae Interoperability Exchange Tests (MINEX). In 2008, Common Biometric Exchange File Format (CBEFF) – wrapper around biometric data by NIST.

Tests underway include:

- NIST Iris Exchange (IREX08): Objectives: support development and interoperability of iris images, establish iris images as the primary exchange format. Examine storage format for iris data and push developers into implementing ISO standard implementations. Establish compact image formats. Evaluate state of the art iris recognition performance. See: http:iris.nist.gov/irex
- Multi Biometrics Test and Evaluation (MBTE): Look at potential for iris or face use in maritime scenarios. Compression of photographs used in ePassports at DHS. Do conformance to capture standards and quality assessments and human factors. Evaluate the potential for iris and/or facial biometrics for use in pedestrian/maritime scenarios.
- Multi-Biometrics Evaluation (MBE) 2009: Follow-up to the Multiple-Biometrics Grand Challenge 2008. Tests to be performed by NIST using code provided by developers. Run against larger,

sequestered data sets. Summer 2009 Staggered start of three tracks: Portal and Video, Executable, Based on FRVT 2006, ICE 2006, and MBGC, Still face track, Operational data, and Submission of SDKs will be an option.

- Multiple Biometric Grand Challenges (MBGC): The MBGC Evaluation Team has designed three challenge problems: Still Face Challenge, Portal Video Challenge and Video Face Challenge. Laboratory (NavLab) certified to perform test on biometric equipment. Lab should be operational this year. Exciting development. First application is airport access control.
- Qualified Products List (QPL) of Biometrics Products: FBI's Certified Products List (CPL) for Fingerprint scanners/card readers, TSA QPL for Biometric Airport Control Systems, Approved Product List for FIPS (201) PIV. FIPS 201 (Federal Information Processing Standards Publication 201) is a USG standard that specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors.

Moving forward, a groundbreaking USG-wide standards selection process is now in place to align USG-wide standards. This is a great step forward. Agencies go through standards and can incorporate into their acquisitions processes. Can audit for compliance. Augmenting the existing USG Conformity Assessment capabilities in support of the recommended standards is now underway. Registry will be updated as new standards emerge or older ones become obsolete.

B. Mr. Ken Martin, Past President, International Association for Identification

HSPD-24 discussion focused on various references to interoperability. Funding is only mentioned once in the HSPD. Mr. Martin discussed HSPD-24 from a state and local perspective, where there is a divergence of law enforcement and DoD missions. Law enforcement needs to achieve criminal prosecution and meet the challenge of court unlike DOD which is intelligence focused. In state and local domains, there are 18,000 state and local law enforcement entities with approximately 800,000 law enforcement officers. Police, chiefs, sheriffs will not give up their domain.

The implementation of HSPD-24 poses several challenges. On compatibility, HSPD-24 calls for compatible methods and procedures but what is the incentive to do this? The directive does not impose requirements to state and local law enforcement and it does not provide new authorities to any agencies. Federal agency databases contain only what they receive. Funding is only mentioned once in the HSPD. Fingerprints are the biometrics base upon which to build but this is not a solid base. There are pre-existing problems. AFIS has its own database structure and algorithms. Interoperability does not work at the state level because information is over classified. If information crosses state borders, no more control, therefore many entities are reluctant to pass data on. There are legal mandates as well including groups, watchdogs, mandates from USG and lobby not to change state law. Funding sent to state and local increases competition on who gets what amount of money. Often, work is not carried out due to lack of manpower to maintain the database.

Local law enforcement issues with collections include when a person is arrested, what goes into a database, and the need for rapid info on person. Fingerprints ink vs. electronic is also a challenge. Locals use cards that don't make it into the databases. DNA categories of crime, time of arrest vs. conviction vs. conditions of release all require database updates. State AFIS are not interoperable nor compatible. In 1995, predictions were made that all AFIS were interoperable. In 2008, this remains the case and change is slow moving. AFIS not a standard database, it is decentralized, and 30 years old. A directory of users is unavailable. The good news is that CODIS is interoperable. Laws are different in each state. For example, wire tap laws differ in many states and conflict at the federal level.

Federal IAFIS has 56M records. NGI will include palm and scars, marks and tattoos. Interoperability is over 10 years. Vendor's best algorithms, search hit rates, law enforcement is reluctant to give up. Accuracy needs to be maintained and one way to do this is to resolve image quality issues.

Resource Issues include workload management where units run 24/7 and hardware/personnel costs are high but resources are thin. To be successful, states need resources for personnel and hardware, MOUs for standardization, and increased connectivity and networking.

C. Dr. Stephen Elliot, Associate Professor of Industrial Technology, Purdue University
How can academia get involved in HSPD-24? Academia can play an active role in a variety to was including: participation on standards, testing and evaluation of products, working with certification bodies, training (external and within the curriculum), testing effectiveness of standards, and play an advisory role for those that need to implement standards. When creating curriculums that involve standards, some curriculums must be replaced, it cannot simply be added. Dr. Elliot focused on many issues surrounding fingeprints, their sensors, and their scanners.

D. Dr. Marios Savvides, Director of Biometrics, CyLab
Dr. Savvides will reiterate much of what Dr. Elliot described with regards to the contributions academia can make in the realm of biometrics and the implementation of HSPD-24. Main focus is face and iris. How can we enhance collected images?

This discussion kicked off with results of tests conducted on facial images to compare the verification rates of images (performance) to tweak algorithm performance. (FRGC is the testing effort). How do we move to consider different face poses and poor quality images that are not megapixel imges? How does one leverage existing infrastructure to deploy effective biometric collection and matching equipment while preserving matching performance? Carnegie Mellon database of facial images provides images of off-pose angles, various facial expressions, and different levels of lighting. Analyzing these variations in facial images allows academia to baseline problems in matching performance. Facial expression analysis. Pose correction using symmetry…

3D morphable models (2D → 3D) From 2D images, 3D images are generated that can be used for matching. Awesome technology for many applications! Iris Sarnoff iris on the move portal. Beyond 20 feet, illumination issues arise during collection. Academia is developing and tweaking algorithms for face and iris that can directly contribute to the performance of matching algorithms.

E. Dr. Arun Ross, Associate Professor, Lane Department of Computer Science and Electrical Engineering, West Virginia University
There are a few words that stick out in HSPD-24 with regards to research: storage and sharing. Within academia, discussion focuses on flow of data from sub-systems (functions) within the biometric process. For example, data flowing from collection sensor to matcher to storage and so on. Biometric databases are becoming increasingly populated by multimodal data of an individual. Indexing techniques are needed to restrict the search to a subset of the database for a quick search.

Multibiometric indexing: the fingerprint modality can narrow the number of possible matches and direct the query image to a particular "bin" of identities. In summary, database organization, template security, and sensor interoperability.

Q&A Session
Q: When will the results of the MBGC be published? Also, I hear calls for interoperability, which is not something addressed until much later in a products lifecycle. How does vendor community engage in implementation of standards earlier in the product lifecycle?
A: It will be quite a while, fairly soon. Agree with second question. Vendors are need to be involved in the standards. Early in the process, companies don't want standards b/c they want to maintain a competitive edge. However, in the long run it is in vendor's best interest to implement standards. Standards are difficult o link to the bottom line of a company. Mr. Brad Wing provided a real world anecdote about the importance of building consensus on passport chips with big manufacturers.

Combination of laboratory and operational testing was crucial in getting the systems conformant to standards.

International Panel Discussion

Key Issues

- Privacy

A. Mexico, Mr. Carlos Raul Anaya Moreno, Director General, National Register of Population and Personal Identification

The Identity Service Mission can best be explained with a comparison to a three legged stool. The three legs are legal identity, living identity, and biometric identity. Legal identity: If there is no legal identity, the chair becomes weak and won't deliver security and trust. Examples of this are voting, or police control. Living identity: Vulnerability of personal data confidentiality, which happens when sold by the private sector without the intervention or audit of public sector. Biometric identity: Lacks physical identity, allows for identity fraud, multiple identities and changeable identities. When one of the legs of the identity service stool is missing or one focus is stronger than other legs – identity service is unbalanced and problematic. Mexican systems use the standards ANSI/NIST ITL 1-2007 Part 2: 2 iris, 2 face, and 10 fingerprint records.

Objectives of the Identity Service Mission: Include guarantees to the right to identity, certify Mexican citizenship (Mexican Constitution, 36 Article), comply with the Universal Declaration of Human Rights (Article 6), strengthen the person's management capacity, simplify and reduce procedures, support full access to the new information society, grant certainty to the economic and social sectors through a document that reliably certified identity; help to generate trust in commercial and financial activities.

Deployment of 100 million ICAO compliant national identity cards over the next 5 years. People are not transactions. We have to break the "transactional paradox" of database processing and retake the concept of Public Service, respecting the dignity of the people and there right to privacy. There is a Mexican website open to the public for all Mexican identities, which includes passports and other personal data elements (name, date of birth, sex). Public website exists for fingerprints as well.

B. INTERPOL, Mr. Joseph Orrigo, Senior CI Advisor, Terrorism and Violent Crime Division

Mr. Orrigo provided an overview of Interpol, which serves as an investigative tool in biometric data sharing. Interpol's mission is to promote and coordinate international police activity. It was created in 1923, it is in 187 countries. The heart of Interpol is its tools: notice program and its data bases, which include the Interpol Criminal Information system (ICIS) and automated search facility (ASF). ICIS is the criminal history of individuals. ASF is the search engine for a number of other databases on various crimes and biometric modalities: DNA profiles, stolen motor vehicles, stolen works of art, child pornography, among others.

US National Central Bureau (USNCB) is located in DC. Project Face Off included a search between Interpol's fingerprint database and the ABIS. 30 individuals were matched. One of which was involved in the 2003 Casablanca bombings. Project Ocean View – involved a matching effort of only names first between Interpol records and databases at DMDC. 10 were identified. Current effort is to match one fingerprint using images stored for CACs. Interpol prints are now converted for matching in IAFIS. New Concept Project is to support DoD and FBI CT overseas efforts: obtain, fingerprints, two way conversion, conduct searches in Lyon, and provide feedback. Approximately 10 minute matches from DoD to Interpol.

Way ahead: IPSG Lyon, expand and upgrade, NIST viewer license, NIST Software, Purchase of V700 Scanners, Increase Storage, virtual data base global system of links, deployment of IRT Team major

events 39. Other New Approaches…Project Oasis in Africa and Mexico focused on building African fingerprint matching capability. Palm prints capability for storage in early 2009. Forensic area, Interpol is working with various countries/disciplines (Canada-explosives, Romania-fingerprint dating, Colombia-artificial prints). Domestic initiatives include Interpol Portal in 2009 and closer coordination with IAFIS-FBI.

Q&A Session
Q: How difficult has it been to obtain the concurrence of all federal agencies to adopt Mexican model? How did you get concurrence between federal, state, and local? Who is bearing the cost of Mexican implementation?
A: Federal program is providing system. No need for state local to implement. 70% of funding is federal, 30% is state/local.
Q: How did Mexico deal with privacy and civil rights groups on identity?
A: All American countries agree with fact that identity is a human right and not an individual/personal right. US needs to put push a more communal perspective. US is the only country in the Americas that doesn't agree with Mexican position on identity.
Q: Identity theft a problem in Mexico?
A: No. Benefits outweigh challenges.
Q: How does Mexico establish the trust of citizens? How costly is the system? Does the Mexican fingerprint system track encounter information?
A: Article 36 of the Constitution requires citizens to provide identity information to the government.
Q: Intrigued about 187 countries involved in Interpol. US doesn't have extradition treaties with each country. How are these things worked?
A: Some of these countries are our enemies. With terrorism, some countries are apt to sharing data. Countries work with Interpol to figure out a way to route an individual to a country that does have an extradition law with the US.
Q: How does Interpol convert fingerprints from one format to another?
A: The process is automated.

Interoperability Panel Discussion

Key Issues
- Interagency Standards for Sharing Data
- Adherence to Standards
- Coordinated Congressional Oversight and Funding

A. Mr. Dirk Rankin, NCTC, Office of Mission Systems Architecture, Engineering & Investment
The National Counter Terrorism Center (NCTC) was stood up in 2004 as a part of the US Intelligence and Reform Act. Cooperative users: rapid and quality collection of unique biometric data. Need standardized collection methodologies. Need to facilitate efficient updating of changes to biometric features (cosmetic surgery, etc.). Biometric data will drive storage solutions geometrically versus biographic-only based designs. Binary data is exponentially larger than ASCII data. Solid certification and accreditation criteria and process is crucial.

Non-cooperative/Uncooperative Users involves issues related to rapid and quality collection at a distance and a growing need for ruggedized sensors worldwide. NCTC phased implementation approach to biometric enabled intelligence (BEI) for counterterrorism. Sharing data is a challenge. Need data standardization, this requires recognition and ownership of problem then adoption of standards. NSTC policy for Enabling the Development, Adoption and Use of Biometric Standards was a step in the right direction. Intelligence Community (IC) Information Sharing Data Standards Coordination Activity is underway through the use of TWPDES, NIEM, & UCORE.

Policy considerations include a way ahead for data exploitation: which model? Bring data to the processor (replication model – high cost) or bring processor to the data (services model – high integrity).

Technology considerations include a way ahead for databases: Relational (Oracle, "pair-at-a-time") or Hierarchal (XML, "many-at-once"). Web 2.0 technologies and cloud computing (shared processing, storage, etc.) should be considered along with service oriented architecture (SOA) constructs. Modernized, fast moving code base – open source, commercial, government should be the goal of USG.

Community considerations must include access and dissemination across security domains. User authentication (LDAP, etc.) must converge on methodologies, standards, formats, security, schedule, cost, performance, risk maintenance, and refresh. Implementation synchronization is hard to do. Unified CONOP required to minimize number of variables, and lower cost. How to integrate Vertical/Horizontal paradigms. Vertical is top-down, policy and budget. Horizontal is peer-level stakeholder implementation.

B. Mr. Paul Grant, Office of CIO, US Department of Defense

Mr. Grant initiated his brief by discussing biometrics within the context of IdM, which includes the tracking of red, blue, and gray forces. IdM also includes tracking all things (objects/people) moving within the Global Information Grid (GIG). Value proposition is the context, strong Identity and Access Management (IdAM) are key to sharing in cyber space and physical access to sensitive locations.

Major move forward in this field was signing policy approving external PKI list. DoD CIO and Northrop Grumman CEO used their respective cards to exchange certificates and exchange sensitive information. This allows external contractors to exchange signed and encrypted emails with DoD. Synchronized Pre-deployment and Operational Tracker (SPOT) is used to track contractors who end up in an Area of Responsibility (AOR). Partners can expect strong credentialing of our employees and robust access to PKI certificates. EADS has the lead to deploy the same in UK Ministry of Defense (MoD), which will allow cross exchange between US and UK. Most of our coalition partners do not have credentials like DoD.

In summary, strong IdAM are key to information sharing and collaboration. We need a clear, consistent, published course for ourselves and our mission partners.

C. Mr. Paul Garrett, Special Assistant To The Chief Information Officer, Department of Justice

Mr. Garrett led off with "Aren't biometrics Really just data?" Mr. Garrett strives to be a mouthpiece for activity in the interagency sharing initiatives. Issues related to sharing need to be elevated within various agencies. Sharing becomes more of a policy and funding problem and less of a technology issue.

Impediments: Congressional funding and oversight is currently stove-piped. How do we as a community push more Congressional oversight? How do you get the attention of the policy makers? Agencies leave critical work on sharing to the techies. No one likes standards to be mandated in a program. Competition is a good thing in markets but not necessarily in government.

The importance of NGI should not be understated. This program has the potential to serve many USG needs. CJIS has a history of service and it possesses the ability to support USG biometrics activities in the long term. Universities (WV & Pitt) and the private sector will need to play a bigger role along with the expanding role of DoD.

USG enterprise must be a federated system with a minimal amount of matching databases. How many matching algorithms does the USG really need? Most of the technical issues have largely been figured out.

Challenges with US-VISIT: Segmentation issue – criminal in IAFIS but criminal and civil information in IDENT. MOUs with others are impacting FBI and FBI customers without realizing the potential damage. Not following Guideline 4. Without exit pushing more work on FBI systems. Keeping data up to date, especially expunged records (2 systems vs. 1 system) audits are slow and expensive.

Concluding Thoughts: Can't separate biometrics from other sharing efforts, can't fund biometrics separately, standards are good and needed. It's a complex issue that requires policy makers to pay attention as it touches: access, privacy, and safety of the homeland.

D. Mr. Thomas Lockwood, Senior Advisor, Screening Credential Office, US Department of Homeland Security

Q&A Session
Q. What is the architecture for sharing attributes within a FIPS 201 framework. Need to rely on trust, need to use standards.
A. How do we change digitized decisions and exchange that with partners? How does that identity and supporting information move beyond the federal architecture? Biometrics can be added into this process to help out.
Q: Didn't hear much about integrating biometrics into the PKI, logical, and physical access spaces?
A: Credentialing and use FIPS201, use of biometrics on the card. Biometrics is bound to the identity.

3. Consolidated List of Key Issues

NDIA tracks the progress of key issues facing the biometrics and identity management arena. These issues will be tracked periodically throughout the year. At the next Biometrics Conference, NDIA will report on the status of each issue.

#	Key Issue Description
1	Consolidation of Congressional Oversight and Budgets
2	Interoperability: Procurement and Implementation of Biometrics Equipment that Adheres to Biometric Standards
3	Coherent Policy Across the USG Governing the Use of Biometrics
4	Unified USG Conformity Assessment Program for Testing Conformance to Biometric Standards
5	Privacy: Ability to Protect and Expunge Data

INTERPOL - ICPO
International Criminal Police Organization

BIOMETRICS CONFERENCE

Joe Orrigo, Senior CI Advisor
Interpol – USNCB Terrorism/Violent Crime Division

Jan 2009

Interpol's Mission

- Created 1923
- Promote and Coordinate International Police Activity
- National Central Bureau –187 Countries
- Identify, Prevent/Suppress Crime

UNIQUE TOOLS

- Notice Program

- Data Bases

  Interpol Crim Information System (ICIS)

  Automated Search Facility (ASF)

Data Bases

- DNA Profiles - 70,238 profiles
- Stolen Motor Vehicles – 3.9 million
- Stolen Works of Art – 31,000 images
- Child Pornography – 516,000 images
- Weapons - 5,000
- Stolen Documents – 15.5 million
- Fingerprints - 80,000

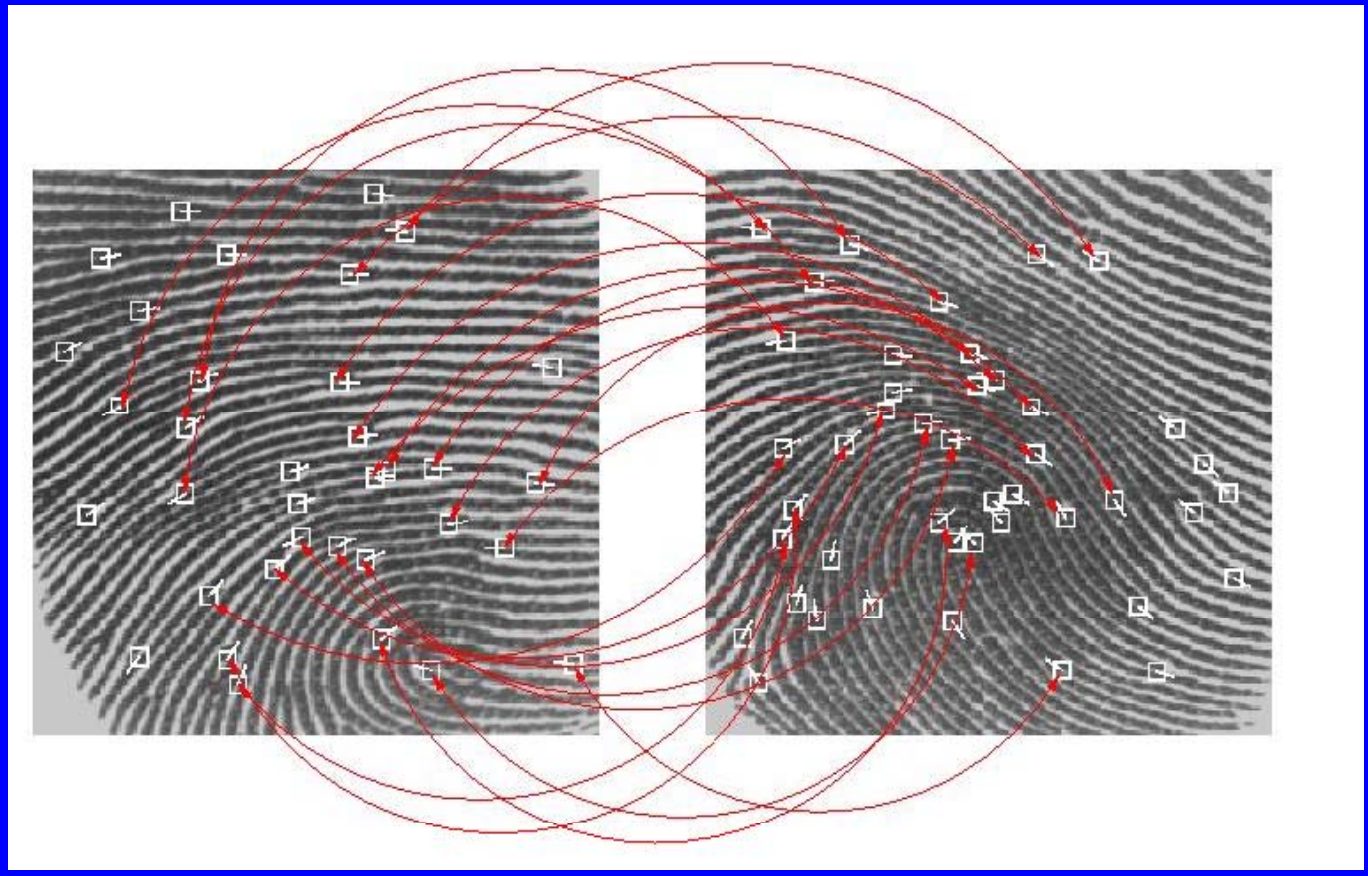
USNCB

- Component of Department of Justice
- Co-Managed by DOJ and DHS
- Central Point of Contact in US
- Approximately 70 people
- 17 Agencies
- 4 Investigative Divisions

USNCB Terrorism Initiatives

- Project Face-Off
- Project Ocean View
- New Support
- IPSG

Project Face Off



Project Ocean View

Interpol Fingerprint Process

Cases to U.S.

Interpol Countries Leads

I/247

USNCB

Convert Prints

FBI CJIS

- CJIS IAFIS Terminal –Time reduction

New Concept Project

Support DoD and FBI CT Overseas Efforts

- Obtain Fingerprints
- Two Way Conversion
- Conduct Searches in Lyon
- Provide Feedback

Interpol Fingerprint Process

New OP

DoD Forces → DoD BFC

DoD BFC → CJIS

CJIS → FBI Checks

CJIS → USNCB

USNCB → IPSG Lyon

USNCB → Conversion

IPSG Lyon → Fingerprint Bank

Fingerprint Bank → Checks

Checks → Results

Conversion → Results

Results → CJIS

Results → USNCB

IPSG Lyon

- **Expand and Upgrade**
  - **NIST Viewer License**
  - **NIST Software**
  - **Purchase of V700 Scanners**
  - **Increase Storage**

- **Virtual Data Base –Global System of Links**
- **Deployment of IRT Teams –Major Events 39**

Other New Approaches

- **Project Oasis**
  - **Africa**
  - **Mexico**
- **Palm Prints – Early 2009**
- **Forensic Area**
  - **Canada –Explosives Program**
  - **Romania –Fingerprint Dating**
  - **Colombia- Artificial Prints**

Expand USNCB

Direction USNB

- Domestic

  -Initiatives

  -Interpol Portal -2009

  -IAFIS -FBI

INTERPOL

Questions?

National Counterterrorism Center

Office of Mission Systems

NDIA Biometrics Interoperability Panel

Dirk Rankin
28 Jan 2009

Overview

- Definitions
- Challenges: Collection, Storage, Use & Analysis, Sharing
- Considerations: Policy, Technology, Community
- Summary

Definitions*

- **Biometrics**: the measureable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition

- **Interoperability**: the ability of two or more systems or components to exchange information and to use the information that has been exchanged

* NSPD – 59 and HSPD –24, 5 Jun 2008

Challenge: Collection

- Cooperative Users
  - Rapid & quality collection of unique biometric data
    - Fingerprints, Iris Scans, Facial Features, DNA, etc.
  - Need standardized collection methodologies
    - Streamline data format translation and archiving for better matching
    - Facilitate efficient updating of changes to biometric features
      - Cosmetic Surgery, Facial Hair, etc.

- Non-Cooperative / Uncooperative Users
  - Rapid & quality collection of unique biometric data *at distance*
  - Growing need for ruggedized sensors worldwide
    - Housings/profile, power, weight, computation, communications
    - Complex collection environments; automation
    - Narrow collection windows

Challenge: Storage

- Biometric data will drive storage solutions geometrically vs. biographic-only based designs
  - PetaByte level depending on collection resolution, number of samples, number of entities
  - Data format compatibility with current production systems to enable efficient operational use within O&M budgets
- Solid Certification & Accreditation criteria and process is crucial
  - Accreditation officials from all stakeholders share equities
  - Must protect U.S. Person's data from unauthorized access
  - Must provide assured access control for authorized users within IC and LE communities respectively
  - Must provide assured access control for those entities authorized for both IC and LE datasets
- Robust backup storage is mission essential
  - Many biometric data collections will be one-time events
  - Crucial component of Continuity of Operations / Disaster Recovery

Challenge: Use & Analysis

- NCTC phased implementation approach to biometric enabled intelligence (BEI) for counterterrorism:
  - Phase 1:
    - Receive, ingest and forward to the TSC nominations of KSTs to include biographic data, facial images and biometric reference numbers
  - Phase 2:
    - Receive and store nominations of KSTs to include biographic data, facial photos, raw fingerprint image files, raw iris image files and biometric reference numbers
    - Introduce CT Data Integration Layer (CTDIL) capability
    - Coordinate and implement standardized electronic nomination format (including associated biometrics) to enable automated ingest into TIDE
  - Phase 3:
    - Search / match raw biometric files against existing TIDE holdings using CTDIL as data service capability (SOA based)
    - Distribute to TSC a comprehensive terrorist identity record

Challenge: Sharing

- Provide assured access across security domains
  - Biometric information, once stored within TS/SCI domain (even if unclassified), generally stays in that domain
  - Maximizing biometric information sharing requires:
    - storing data at lowest permissible security domain, then enabling secure access mechanisms for users operating within higher domains
    - storing data at highest security domain, then enabling secure access from lower domains
  - Multilevel security platform-based solutions; verified mandatory access control model

- Data standardization ownership and adoption
  - NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards
  - IC Information Sharing Data Standards Coordination Activity
    - Terrorist Watchlist Personal Data Exchange Standard (TWPDES)
    - National Information Exchange Model (NIEM)
    - DoD – DNI Universal Core (UCORE)

Policy Considerations

- …AG and DNI shall ensure that policies and procedures for the consolidated terrorist watchlist maximize the use of all biometric identifiers
- …DNI shall maintain and enhance interoperability among agency biometric and associated biographic systems, by utilizing common information technology and data standards, protocols and interfaces
- …DNI shall ensure compliance with laws, policies, and procedures respecting information privacy, other legal rights, and information security
- …DNI shall ensure that biometric and associated biographic and contextual information on KSTs is provided to NCTC and TSC
- …DNI shall coordinate the sharing of biometric and associated biographic and contextual information with foreign partners

- **Data Exploitation Way Ahead: Which Model ??**
  - Bring Data to the Processor (replication model – high cost)
  - Bring Processor to the Data (services model – high integrity)

Technology Considerations

- Database
  - Relational (Oracle, “pair-at-a-time”)
  - Hierarchal (XML, “many-at-once”)
- Web 2.0 technologies
  - Cloud Computing (shared processing, storage, etc.)
  - Service-oriented Architecture (SOA) constructs
- Modernized, fast moving code base
  - Open Source, Commercial, Government
- Access and dissemination across security domains
  - User authentication (LDAP, etc.)
  - Approved, accepted, adopted Protection Level (PL) capabilities for implementation of sharing paradigm

Community Considerations

- Must converge on methodologies, standards, formats, security, schedule, cost, performance, risk, maintenance, refresh…
  - Implementation synchronization hard to do
- Unified CONOP required to minimize number of variables, lower cost, increase potential for success
  - Policy authorization, support, resourcing essential
  - Long-range mindset
- How to integrate Vertical and Horizontal paradigms
  - Vertical: top-down policy, budget…
  - Horizontal: peer-level stakeholder implementation…

Summary Points

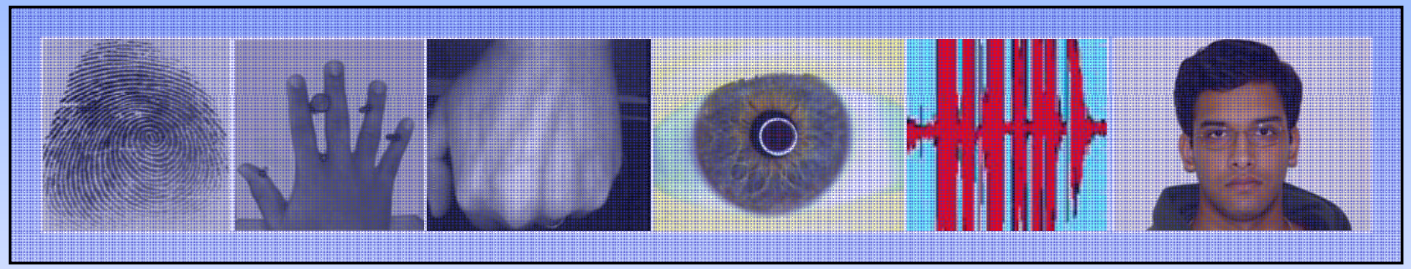
- NCTC recognizes the value of biometrics in identity discovery
- Current state: working to incorporate biometrics into the USG's central repository for KSTs
  - Means a more comprehensive repository for analysts and better watchlisting support to screeners
- Effective biometric enabled intelligence (BEI) implementation requires new thinking and strong commitment across stakeholders

BACK-UP

Watchlisting: Legal and Policy Framework

- IRTPA: December 2004
  - NCTC to serve as the central and shared knowledge bank on known and suspected terrorists (KSTs)
- HSPD-6/TSC MOU: September 2003
  - Development of a comprehensive database of international terrorist identities at the NCTC
  - Creation of TSC to consolidate the governments approach to terrorist screening
  - NCTC as single source of international terrorist data for the TSC's consolidated watchlist database
- Addendum A and B to TSC MOU: August 2004 and January 2007
  - DOD and Treasury added to database sharing community of interest
  - Expands FOUO data identifiers from ~ 7 to 40
- NSPD 59/HSPD 24: June 08
  - Focus on biometrics to further identify KSTs
  - Category of National Security Threats (NSTs)
  - Calls for Interagency Action Plan

HSPD24: Data Organization, Security and Interoperability Challenges



Arun Ross

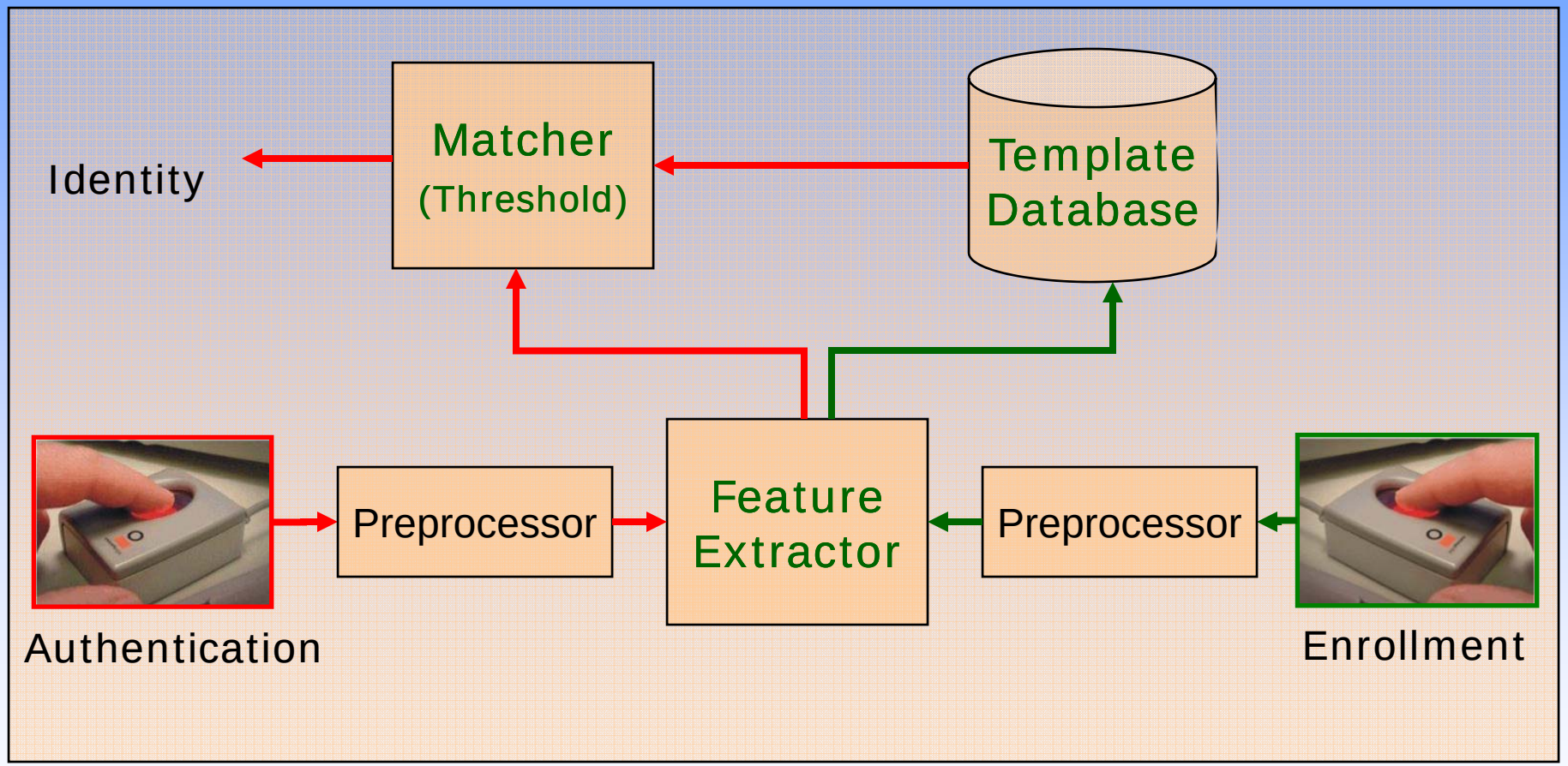
Associate Professor
West Virginia University
Morgantown, West Virginia, USA
Arun.Ross@mail.wvu.edu

http://www.csee.wvu.edu/~ross

HSPD 24

"….use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law."

Biometrics: A Pattern Recognition System



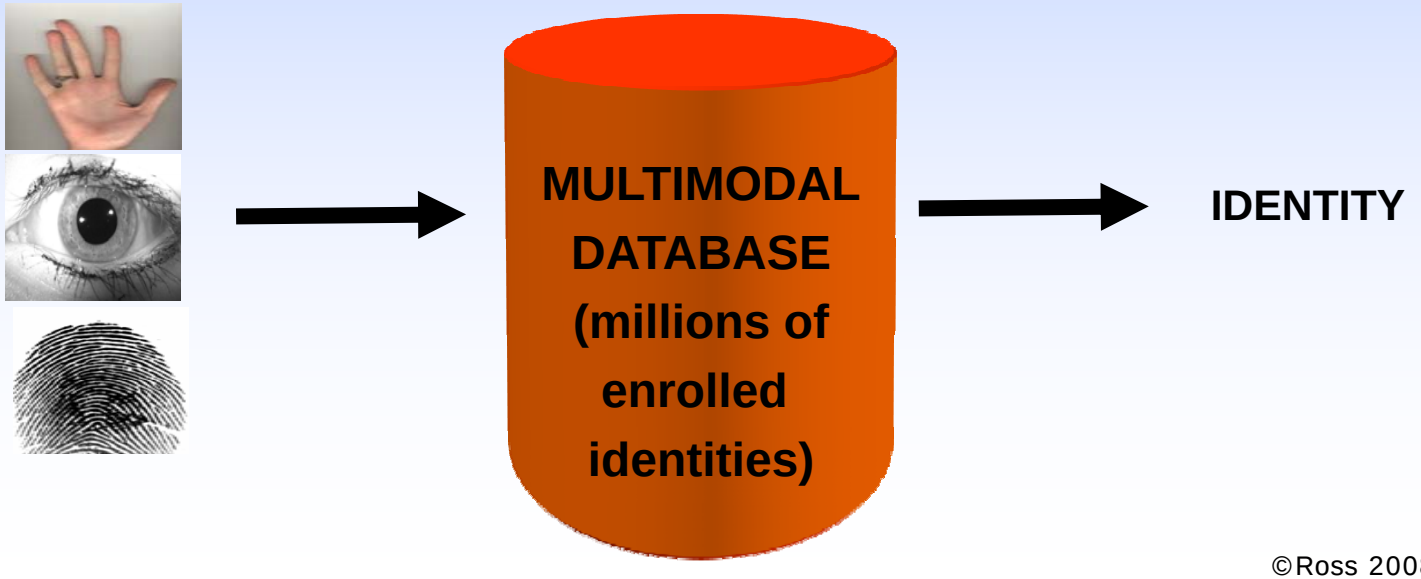
- False accept rate (FAR): Proportion of impostors accepted
- False reject rate (FRR): Proportion of genuine users rejected
- Failure to enroll (FTE) rate
- Failure to acquire (FTA) rate

Multimodal Databases

- Biometric databases are being increasingly populated by multimodal data of an individual
- This data can be categorized as:
  - Biographic/Demographic: age, gender, ethnicity, height, eye color
  - Biometric: fingerprint, face, iris
- Searching through the entire database to retrieve the correct identity is a time-consuming task that significantly impacts the system response time

Search and Retrieve Problem

- Given a suspect's multimodal biometric information (e.g., fingerprint, iris, palm), determine if his identity is present in a large multimodal database as quickly as possible
- Indexing techniques are needed to restrict the search to a subset of the database for a quick answer



Biometric Indexing

Sensor

Feature Extractor

FEATURES

INDICES

Decision

Matcher

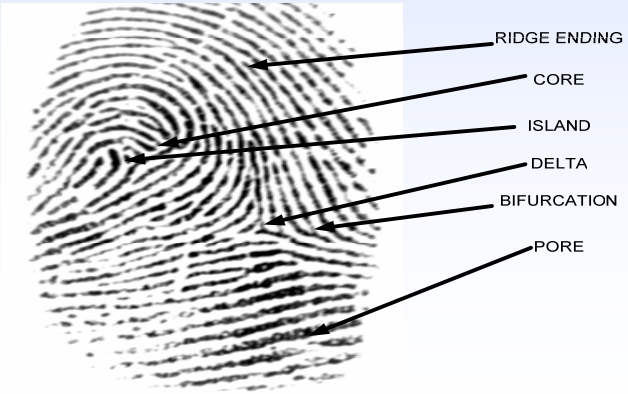
Retrieve Templates

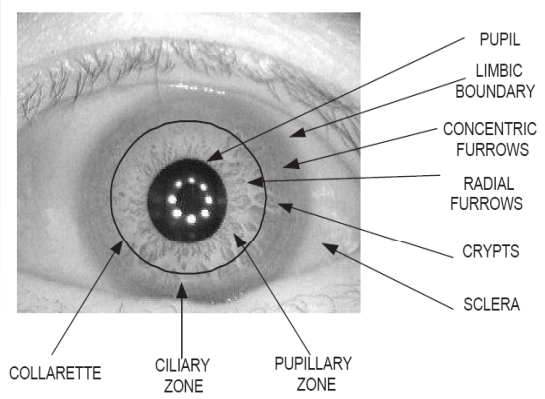
user01 001100...
user02 010011...
user03 100110...

Template Database

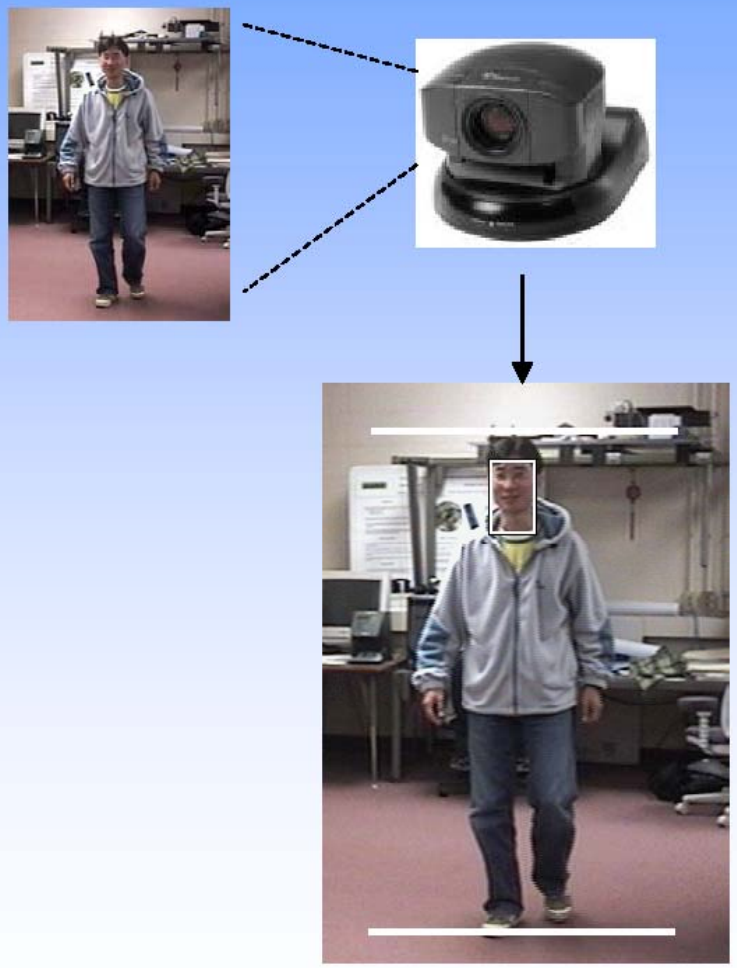
Multibiometric Indexing

- The fingerprint modality can narrow the number of possible matches and direct the query image to a particular “bin” of identities
- Then the iris modality can be used
  - to retrieve the best match from this “bin” of identities
  - cluster the “bin” of identities further in order to further prune the search space





Soft biometric traits



Height: 5.9 ft.

Eye color: black

Gender: Male

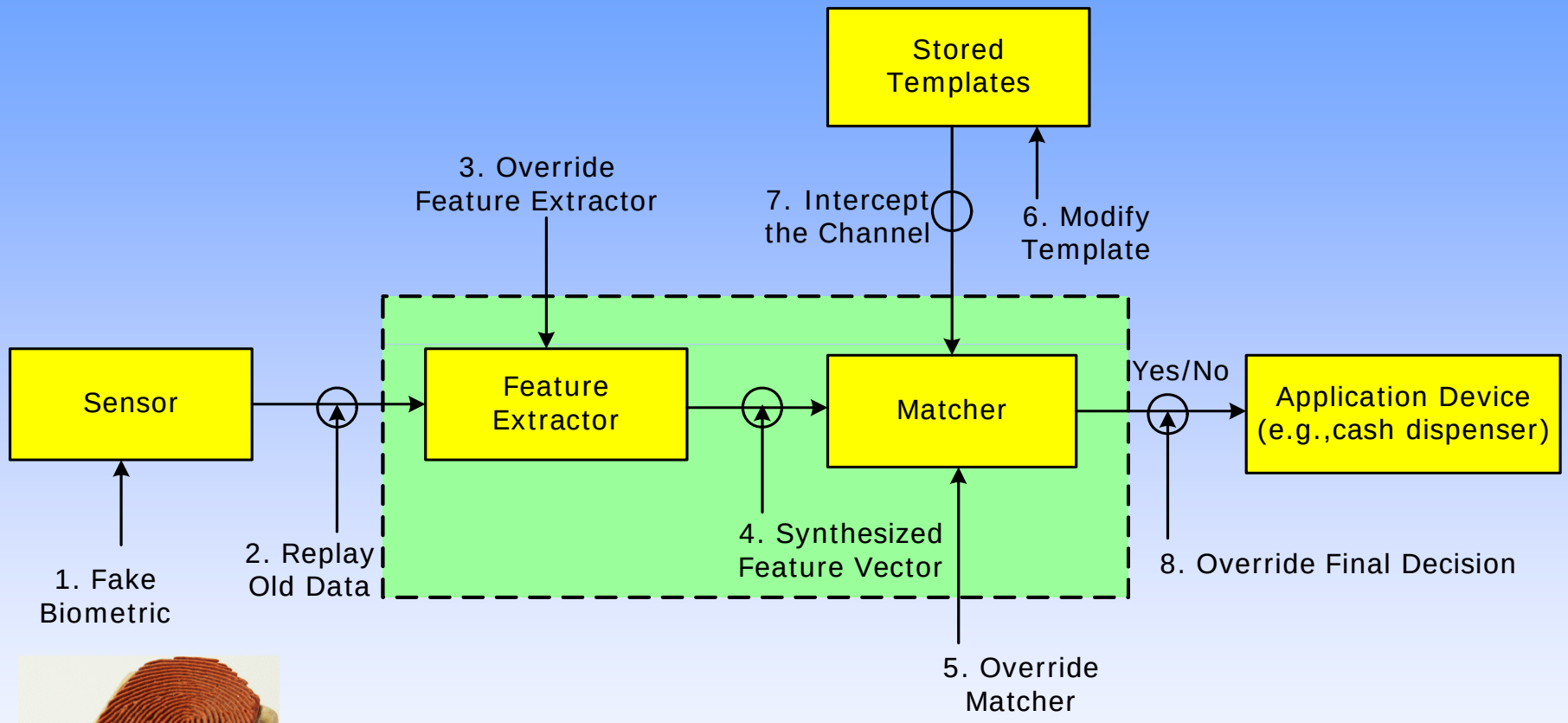
Ethnicity: Asian

Face: LDA Coefficients

Identity: Unsang

Jain et al, "Utilizing soft biometric traits for person authentication", Proc. International Conference on Biometric Authentication (ICBA), Hong Kong, July 2004

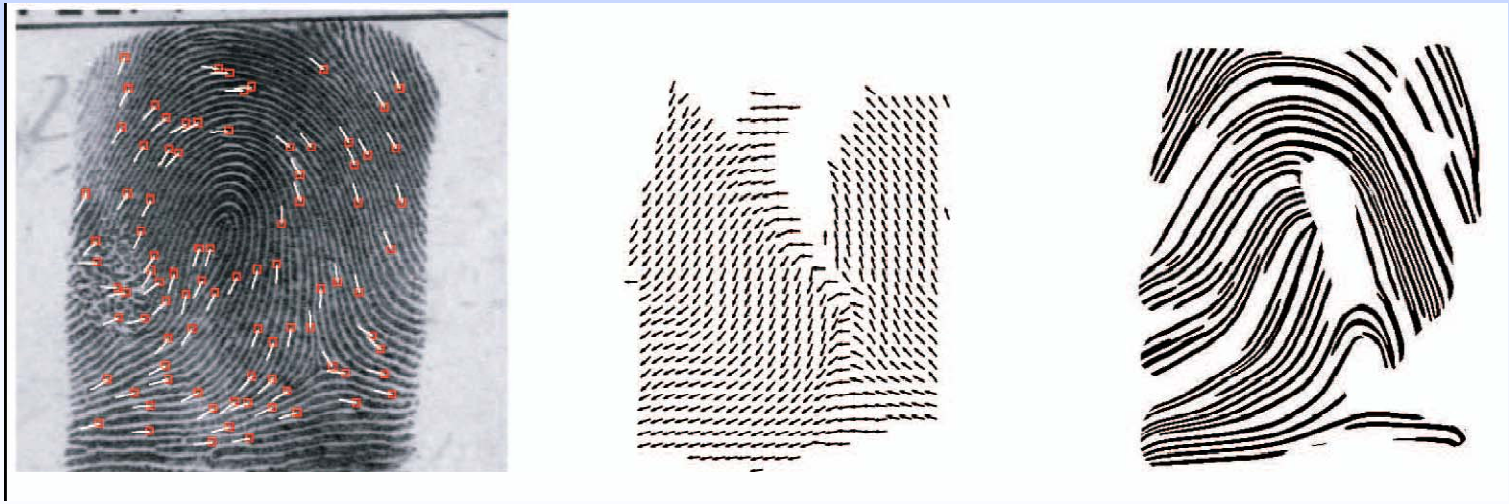
Attacks on a Biometric System



Ratha et al., An Analysis of Minutiae Strength, AVBPA 2001

Template Protection

- A prototype (template) of a user's biometric is stored in a database or a smart card
- Myth: "A true biometric image cannot be created from master template.."
- Biometric template security is critical

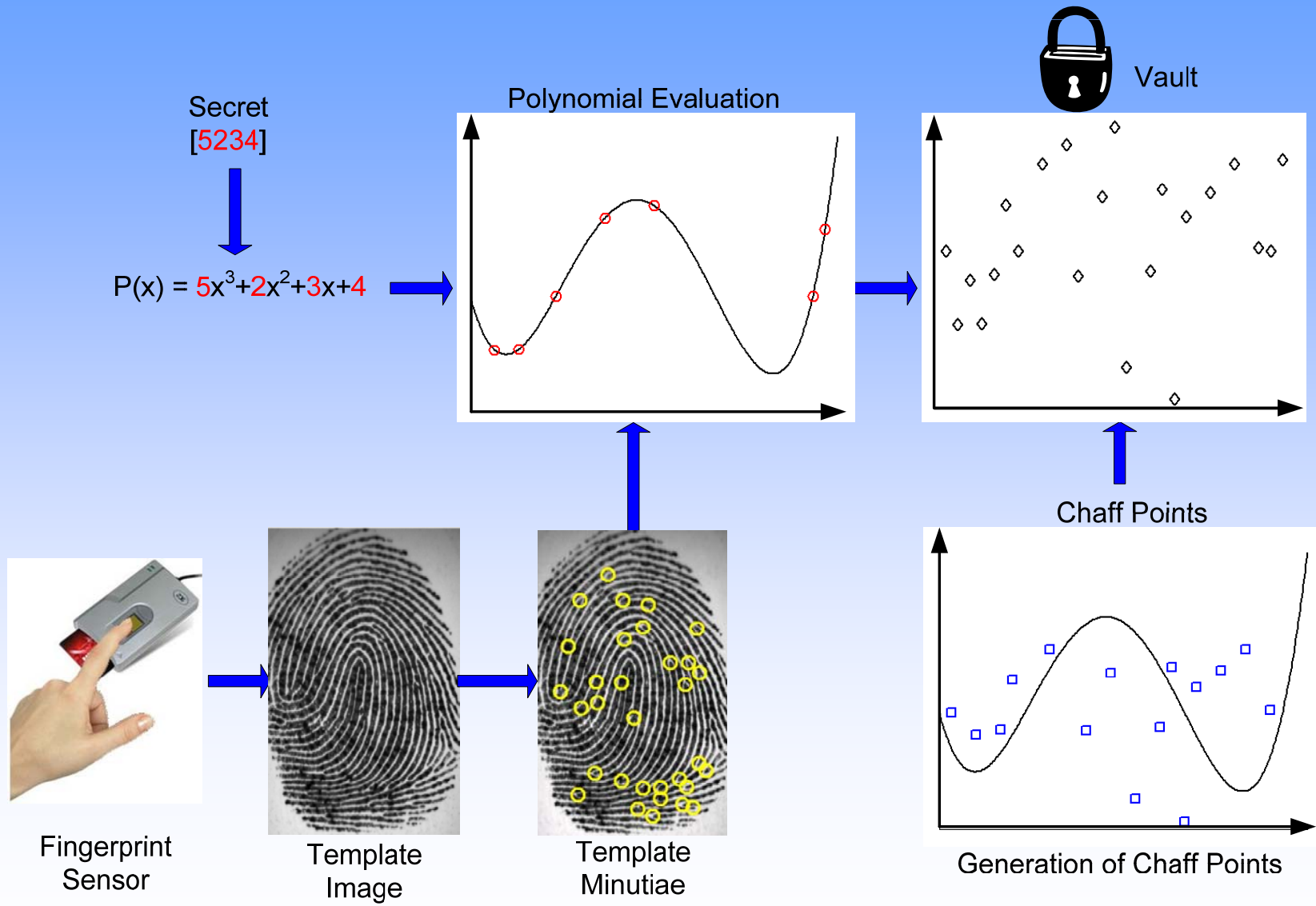


A. Ross, J. Shah and A. K. Jain, "From Template to Image: Reconstructing Fingerprints From Minutiae Points," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 4, pp. 544-560, April 2007.

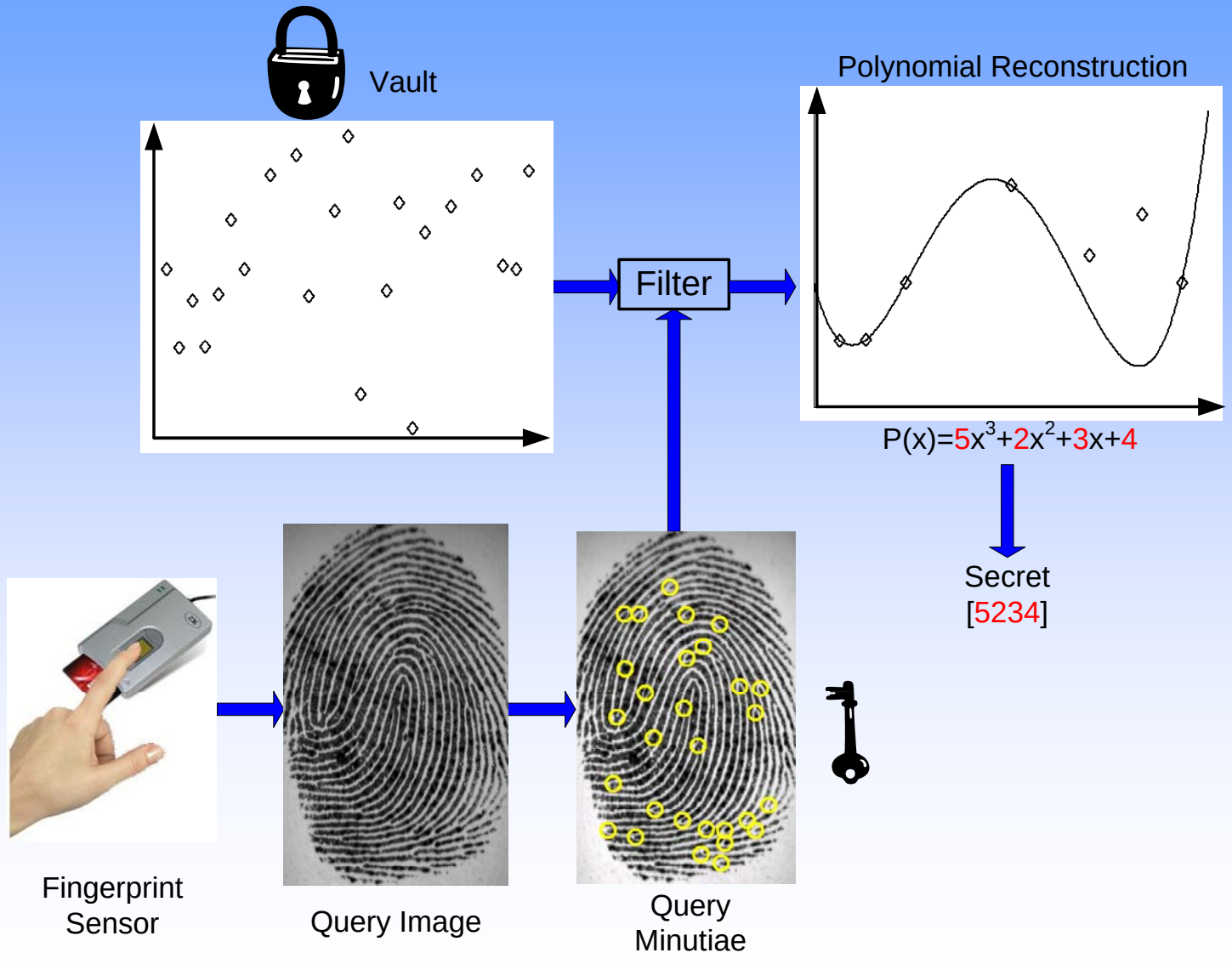
Protecting Biometric Templates

- Encryption
  - Template is encrypted using cryptographic methods
- Steganography
  - Hide the template in a carrier (cover) image
- Cancelable Template
  - Store non-invertible transform of the template
- Fuzzy Vault
  - Template is cryptographically bound to a secret; can be decoded only when matching image is available

Fuzzy Vault



Fuzzy Vault



Sensor Interoperability

Crossmatch Verifier 300

Ethenticator USB 2500

Secugen Hamster III

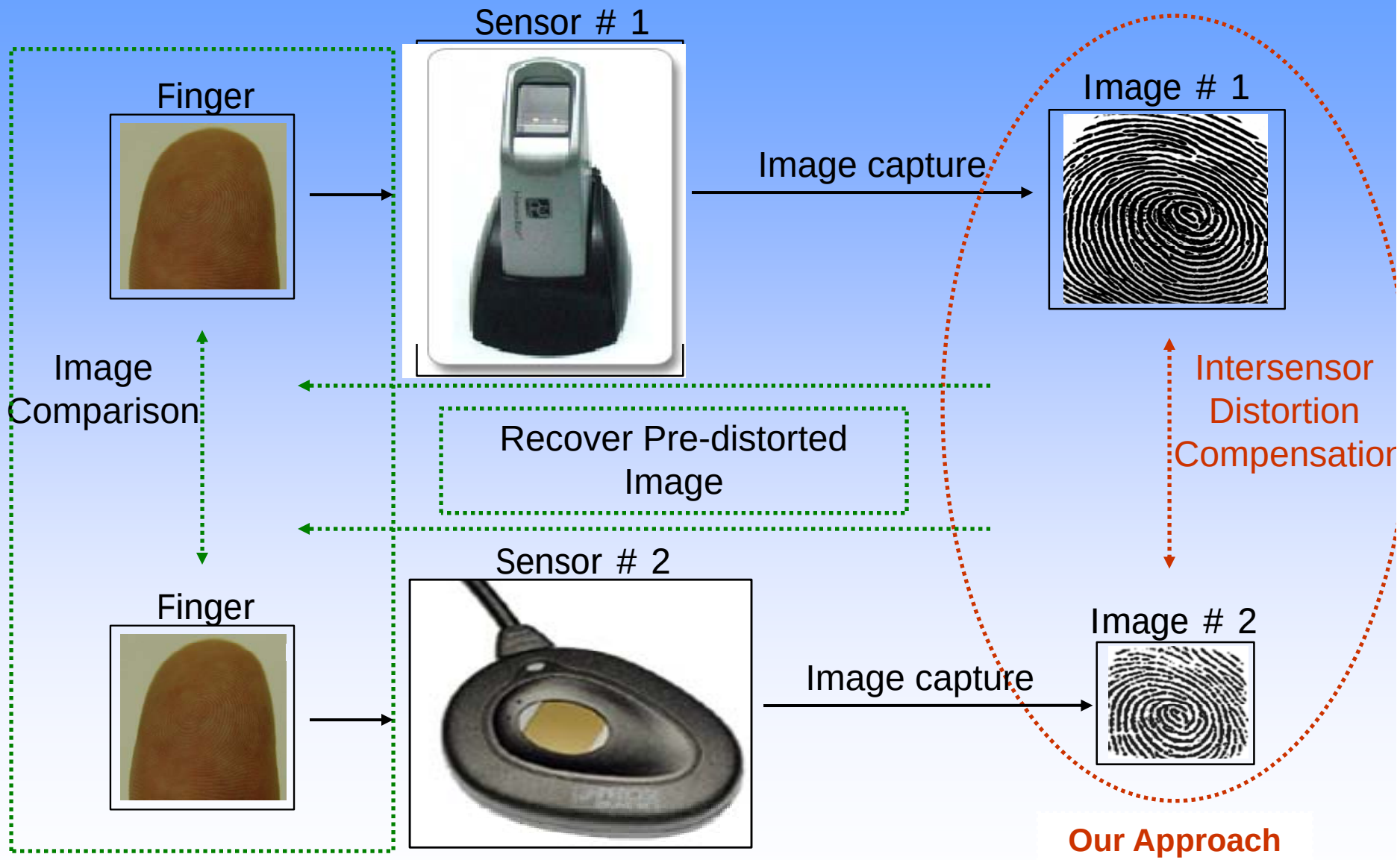
Precise 100AX

Digital Persona U.are.U 4000

Sensor Interoperability

- Can the fingerprint matcher successfully compare two minutiae templates originating from different sensors?

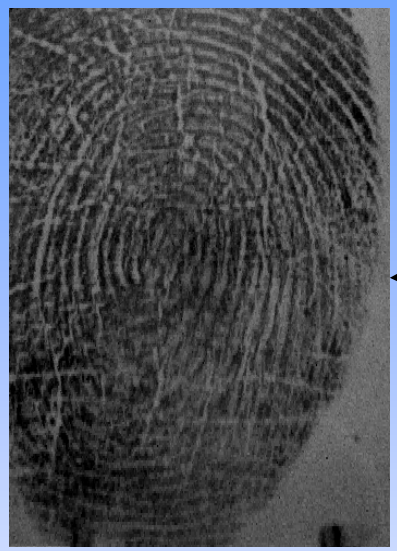
Sensor Interoperability



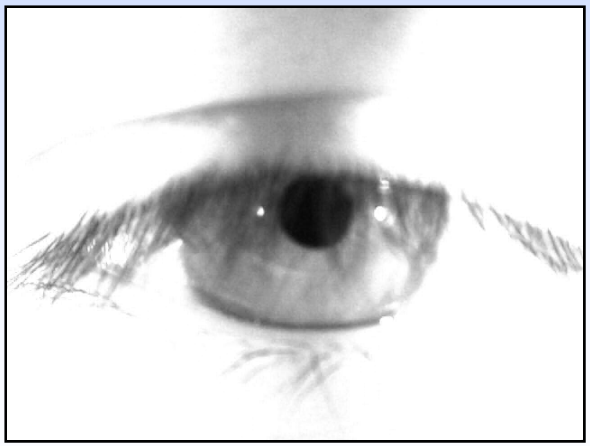
A. Ross and R. Nadgir, "A Calibration Model for Fingerprint Sensor Interoperability", *Proc. of SPIE Conference on Biometric Technology for Human Identification III*, (Orlando, USA), April 2006.

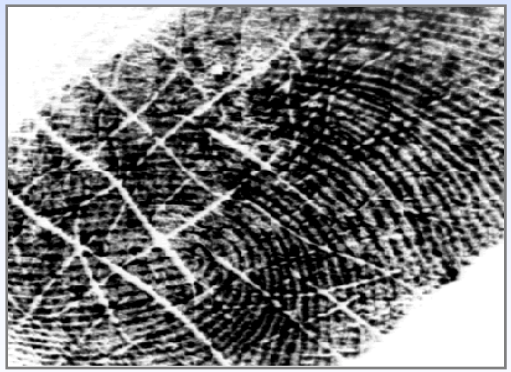
Noise in sensed data

During enrolment



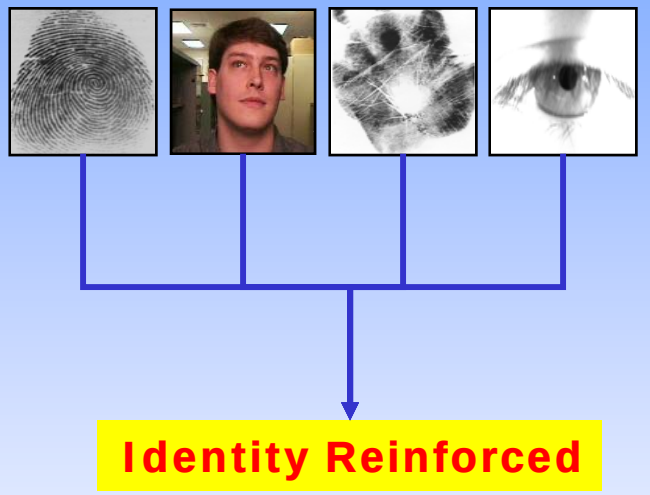
During authentication





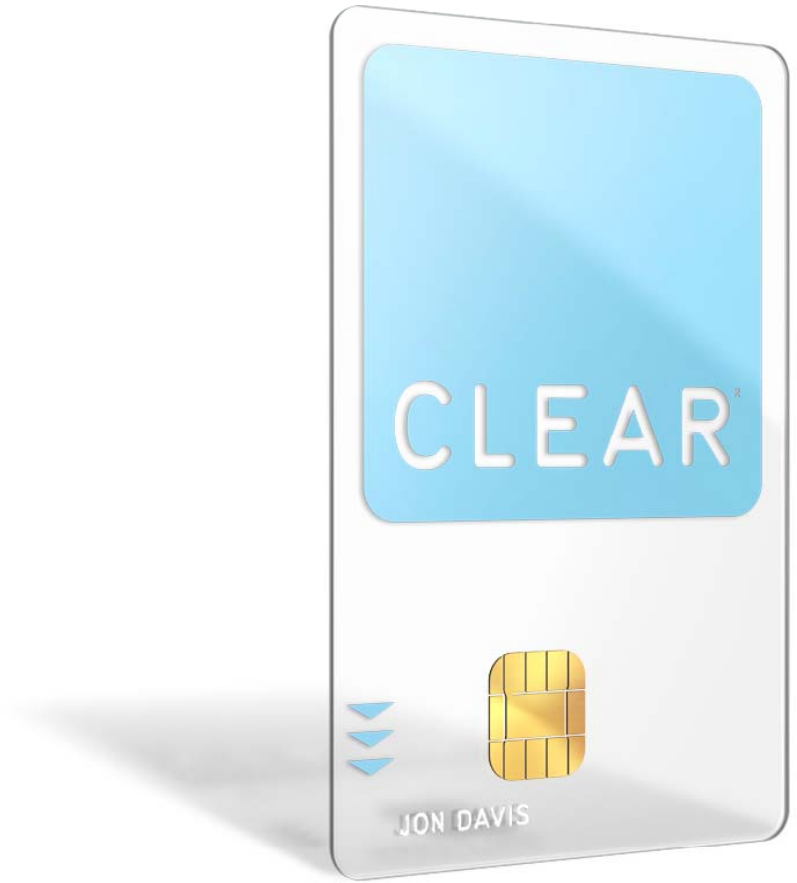
Multibiometrics

- Information fusion in the context of biometrics
- The identity of an individual is reinforced through multiple pieces of evidence
- The use of multiple sources of evidence is especially significant in non-ideal scenarios where individual modalities can not be easily acquired



Summary

- Database Organization
  - Fast retrieval of identities
  - “Missing data” or “noisy data” problem
- Template Security
  - Protecting biometric templates
  - Matching in the encrypted domain
- Sensor Interoperability
  - Match data acquired using different sensors



IMAGINE THE LONG SECURITY LINE WITHOUT THE "LONG" PART.

CLEAR LESSONS LEARNED

JASON SLIBECK, CTO, VERIFIED IDENTITY PASS, INC.

CLEAR

FLY THROUGH AIRPORT SECURITY.

ABOUT CLEAR

- CLEAR IS THE LARGEST REGISTERED TRAVELER PROGRAM OPERATING AT U.S. AIRPORTS WITH OVER 250,000 MEMBERS SINCE JUNE, 2005.
- PARTNERSHIPS ARE ESTABLISHED WITH 20 AIRPORTS AND AIRLINES, PLUS MAJOR MARKETING PARTNERS.
- TECHNICAL INTEROPERABILITY IS ACHIEVED WITH ALL CERTIFIED REGISTERED TRAVELER SERVICE PROVIDERS.
- ALL CAPITAL AND OPERATING COSTS ARE SUPPORTED BY VOLUNTARY MEMBERSHIP - NO COST TO TAXPAYERS OR AIRPORTS.

CLEAR

FLY THROUGH AIRPORT SECURITY.

KEY POINTS

ATTENTION TO CUSTOMER SERVICE CAN RAPIDLY SPEED GROWTH AND SATISFACTION.

INTEROPERABILITY PROVIDES FLEXIBILITY AND ENCOURAGES STAKEHOLDERS.

TRUE SECURITY BENEFITS ARE AN IMPORTANT PART OF THE SERVICE OFFERING.

CLEAR

FLY THROUGH AIRPORT SECURITY.

REGISTERED TRAVELER HISTORY

2004-2005: TSA CONDUCTS LIMITED, GOVERNMENT-SPONSORED RT PILOT PROGRAM

APRIL 2005: ORLANDO INTERNATIONAL AIRPORT ISSUES COMPETITIVE RFP FOR PRIVATE SECTOR KNOWN TRAVELER (PSKT)

JUNE 2005: CLEAR, WINNER OF PSKT CONTRACT, OPENS IN ORLANDO

OCTOBER 2005: WORK BEGINS ON INTEROPERABILITY AND INDUSTRY INPUT INTO FUTURE OF RT IN US

SEPTEMBER 2006: FIRST VERSION OF TECHNICAL SPECIFICATIONS FOR INTEROPERABILITY PUBLISHED

NOVEMBER 2006: TRANSITION FROM ORLANDO PILOT TO NATIONAL, INTEROPERABLE PROGRAM BEGINS

JANUARY 2007: JFK (T7), SJC, IND, AND CVG CLEAR LANES OPEN

JUNE 2007: UNISYS OPENS INTEROPERABLE PROGRAM IN RENO

MAY 2008: UNISYS PURCHASED BY FLO

MAY 2008: ONE MILLION TRIPS MADE THROUGH CLEAR LANES SINCE LAUNCH

JULY 2008: TSA ENDS PILOT AND ENCOURAGES CONTINUED EXPANSION OF PRIVATE SECTOR MODEL

CLEAR

FLY THROUGH AIRPORT SECURITY.

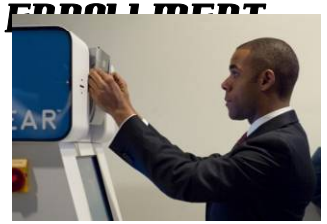
REGISTERED TRAVELER AIRPORTS

FLY THROUGH AIRPORT SECURITY.

CUSTOMER SERVICE: HOW CLEAR WORKS

1 ONLINE ENROLLMENT

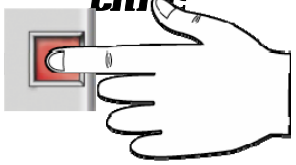
2 IN-PERSON



3 IDENTITY VERIFICATION AND VETTING

4 CARD PRODUCTION AND FULFILLMENT

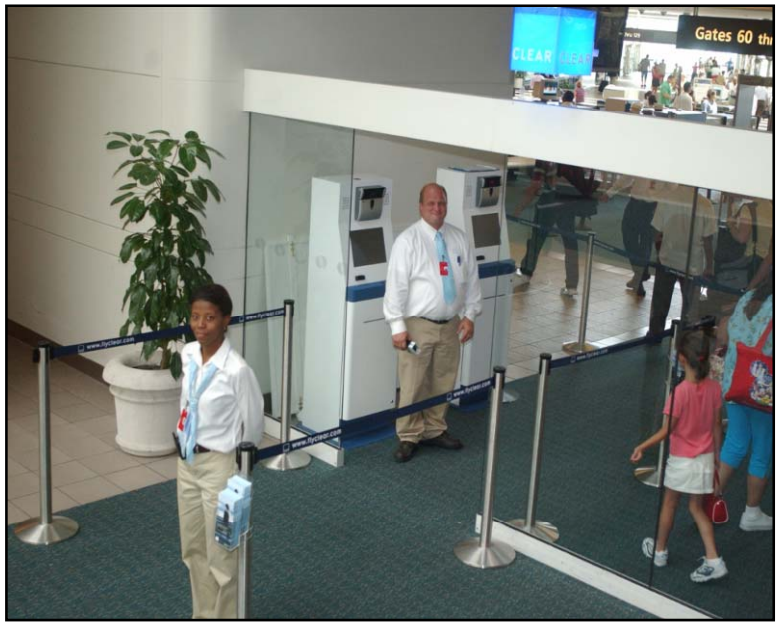
5 VERIFICATION AT THE CLEAR LANE



CLEAR

FLY THROUGH AIRPORT SECURITY.

Customer Service:
Current Benefits of Clear



Top Frequent Flier Frustrations:

- Long lines
- Inability to predict the wait
- Poor customer service

The Clear Solution:

- Members get through in 1 to 5 minutes.
- Members get a consistent, predictable experience at every Clear airport.
- Clear concierge attendants help travelers move faster through the checkpoint.

CLEAR

FLY THROUGH AIRPORT SECURITY.

INTEROPERABILITY: OPEN TECHNOLOGY STANDARDS

FINGERPRINTS

- TEN SLAP PRINTS AT ENROLLMENT
- FOUR FINGERPRINTS ON RT CARD - INCITS 378-2004

IRIS

- OPTIONAL CAPTURE
- RECTILINEAR FORMAT FOR ENROLLMENT AND STORAGE AT CIMS
- UNSEGMENTED POLAR IMAGE FORMAT FOR RT CARD
- COMPLIANT WITH ISO/IEC 19794-6:2005

FACIAL PHOTO

- ANSI INCITS 385-2004
- ISO/IEC 15444 JPEG 2000 IMAGE CODING SYSTEM
- STORED ON CARD, BUT NOT USED FOR AUTHENTICATION

SMART CARD

- US REAL ID ACT FOR TRANSPORTATION IDENTIFICATION
- ISO/IEC 7810, 10373-1, ANSI INCITS 322-2002

CLEAR

FLY THROUGH AIRPORT SECURITY.

INTEROPERABILITY: BEYOND TECHNOLOGY STANDARDS

RTIC Technical Interoperability Specification

- Introduction & Overview
- Concept of Operations
- Biometric Data Management & Use
- System Messaging
- RT Card Model
- System Security
- Conformance Testing Principles

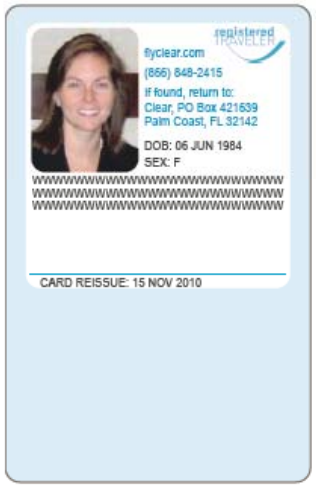
www.rtconsortium.org

FLY THROUGH AIRPORT SECURITY.

SECURITY BENEFITS: CLEAR CARD WITH ENHANCED SECURITY FEATURES

Card Front

Card Back



FEATURES ADDED TO DETER FORGERY AND COUNTERFEITING, PROMOTE CONFIDENCE IN THE AUTHENTICITY OF THE CARD AND FACILITATE DETECTION OF FRAUDULENT CARDS.

IN JUNE, 2008, DHS ACCEPTED CLEAR AS A SECURE IDENTIFICATION CARD ISSUED CONSISTENT WITH DHS STANDARDS.

WORKING TOWARDS HARMONIZATION WITH REAL ID ACT REQUIREMENTS.

TSA CHANGING TRAVEL DOCUMENT CHECKER POLICIES TO ACCEPT CLEAR CARD INTO THE LIST OF ACCEPTED DOCUMENTS AT ALL AIRPORT CHECKPOINTS.

SECURITY BENEFITS: ADVANTAGES FOR AIRPORTS

AS MORE TRAVELERS JOIN CLEAR, THE PERCENTAGE OF PRE-SCREENED, LOW RISK FLIERS GOING THROUGH SECURITY INCREASES.

WITH LOWER RISK TRAVELERS REMOVED FROM GENERAL SECURITY, RESOURCES CAN BE BETTER ALLOCATED.

TECHNOLOGY INNOVATIONS CAN LEAD TO PROCESS IMPROVEMENTS WITH HIGH RETURNS ON THROUGHPUT AND NO INVESTMENT OF CAPITAL.

CLEAR

FLY THROUGH AIRPORT SECURITY.

SECURITY BENEFITS: VERIFICATION KIOSK WITH SHOE-SCANNING TECHNOLOGY

1. Iris camera

2. Receipt Printer
Instructs member on required divesting and communicates alerts to TSA

3. Clear card reader

4. Itemiser
Uses finger sampling technology to detect trace explosives. For future benefits.

5. Fingerprint reader

6. Shoe Scanner
Can detect both explosives and metal below the knee. For future benefits.

CLEAR

FLY THROUGH AIRPORT SECURITY.

KEY POINTS SUMMARY

ATTENTION TO CUSTOMER SERVICE CAN RAPIDLY SPEED GROWTH AND SATISFACTION.

INTEROPERABILITY PROVIDES FLEXIBILITY AND ENCOURAGES STAKEHOLDERS.

TRUE SECURITY BENEFITS ARE AN IMPORTANT PART OF THE SERVICE OFFERING.

CLEAR

FLY THROUGH AIRPORT SECURITY.

POINT OF CONTACT

JASON SLIBECK

CHIEF TECHNOLOGY OFFICER

CLEAR | VERIFIED IDENTITY PASS, INC.

600 THIRD AVENUE, 10TH FLOOR

NEW YORK, NY 10016

212-332-6317

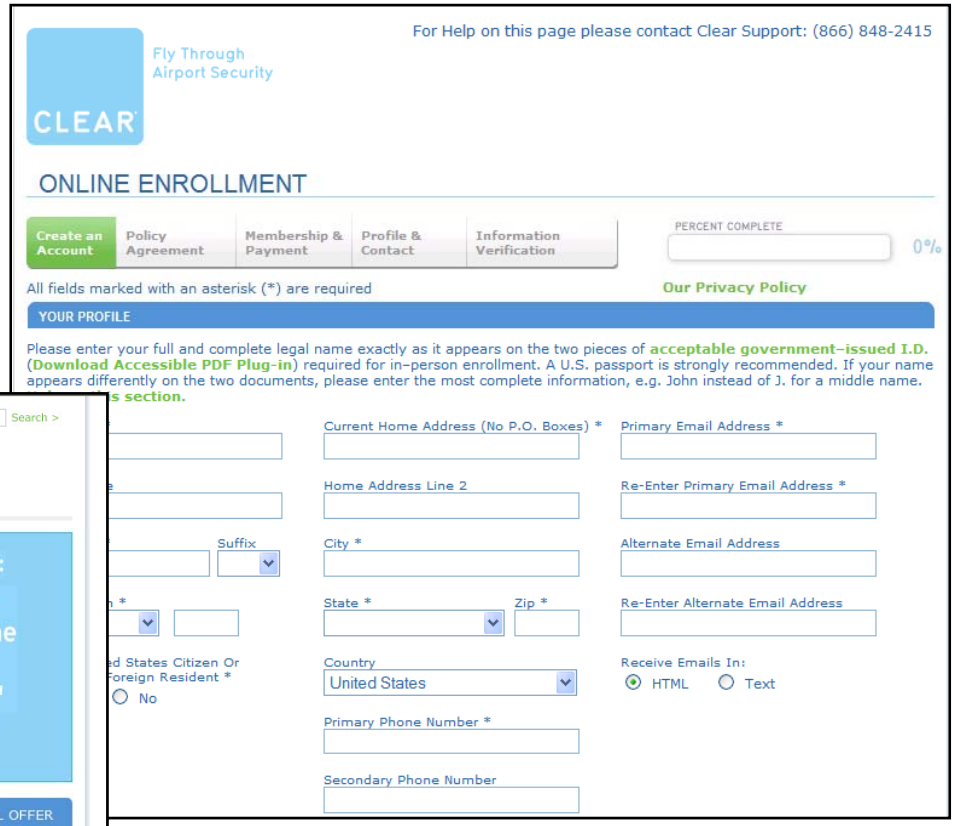
JSLIBECK@VERIFIEDIDPASS.COM

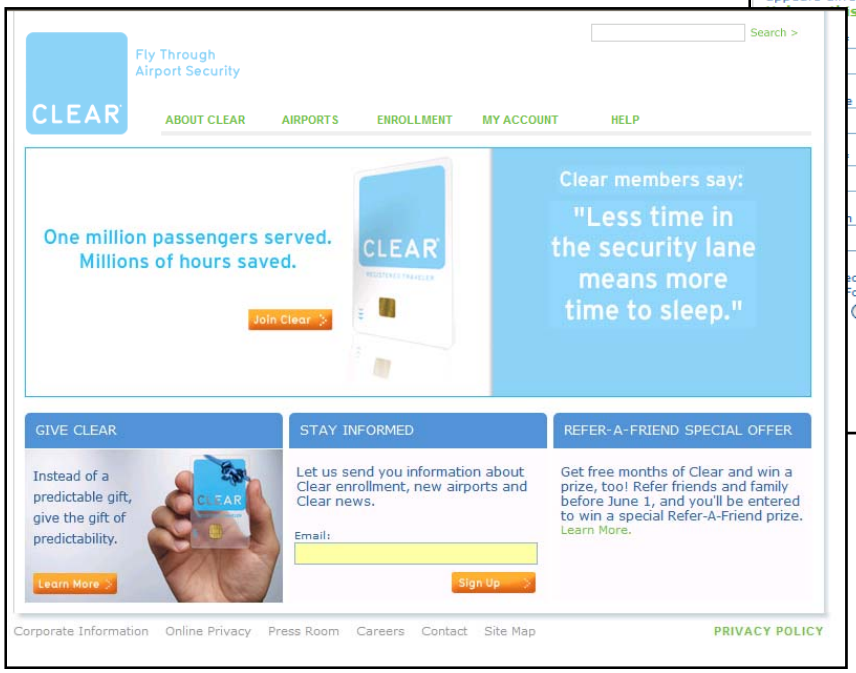
WWW.FLYCLEAR.COM

STEP ONE OF ENROLLMENT: FLYCLEAR.COM

Online Enrollment

- Provide payment information
- Enter Biographic information required by TSA





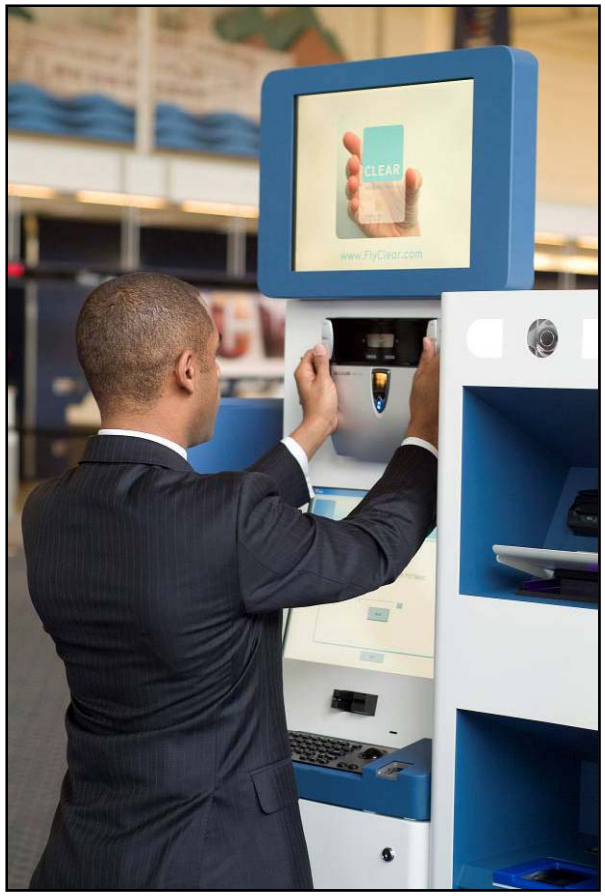
STEP TWO OF ENROLLMENT: IN AIRPORT OR MOBILE ENROLLMENT STATIONS

- During in-person enrollment, a Clear attendant validates the Clear applicant's passport and driver's license, captures images of his or her biometrics, and takes a photo.
- Clear works with the airport or airline to identify appropriate and convenient locations for the Clear enrollment stations.
- Clear has set up convenient mobile enrollment station locations in major metropolitan areas.
- Clear provides mobile teams for convenient enrollment at offices and businesses.

CLEAR

FLY THROUGH AIRPORT SECURITY.

IRIS AND FINGERPRINT CAPTURE AT ENROLLMENT



CLEAR CARD AT THE VERIFICATION KIOSK

The Clear card is inserted into the kiosk and the member is prompted to present either a fingerprint or iris image. The “primary biometric” that members use for identity verification is selected by the member during enrollment.

CLEAR ENROLLMENT KIOSK

- Iris Image Camera: Panasonic BM-ET330
- Photo Camera: Logitech Quickcam Pro 4000
- Viisage iA-thenticate Document Scanner
- Touch Screen Display
- 10-Print Fingerprint Reader: Cross Match ID500
- Single Fingerprint Reader: Cross Match Verified 300 LC
- Canon Flat Bed Scanner
- Receipt Printer

CLEAR

FLY THROUGH AIRPORT SECURITY.

IDENTITY VERIFICATION KIOSK

1. Iris camera

2. Receipt Printer
Instructs member on required divesting and communicates alerts to TSA

3. Clear card reader

4. Fingerprint reader

TECHNICAL SPECIFICATIONS – TSA SPCS

SPCS

•Security, Privacy and Compliance Standards for Sponsoring Entities and Service Providers

•Provides prospective Sponsoring Entities and Service Providers a comprehensive description of TSA's standards for:

- RT Information Systems: Standards for securing information systems transmitting and or holding RT participant data
- Enrollment/ Verification: Process-specific standards for establishing internal controls over participant enrollment and verification.
- Ongoing Compliance: Detailed procedures for demonstrating compliance with the standards.

Biometrics in Private Industry

Fraud Prevention in the GMAT® Exam

Katherine Harman-Stokes, JD, CIPP

Associate General Counsel, Assistant Corporate Secretary, Graduate Management Admission Council® (GMAC®)

Fraud Prevention in the GMAT Exam

Outline

- GMAC and the GMAT exam
- Why biometrics?
- Digital Fingerprints
- Technical and Legal Challenges
- New for 09: Palm Vein Reader
- Biometrics in Europe

What are GMAC® and the GMAT®?

Graduate Management Admission Council® (GMAC®)

- Not for profit, comprised of 160 member schools
- Mission: To create access to graduate business education worldwide

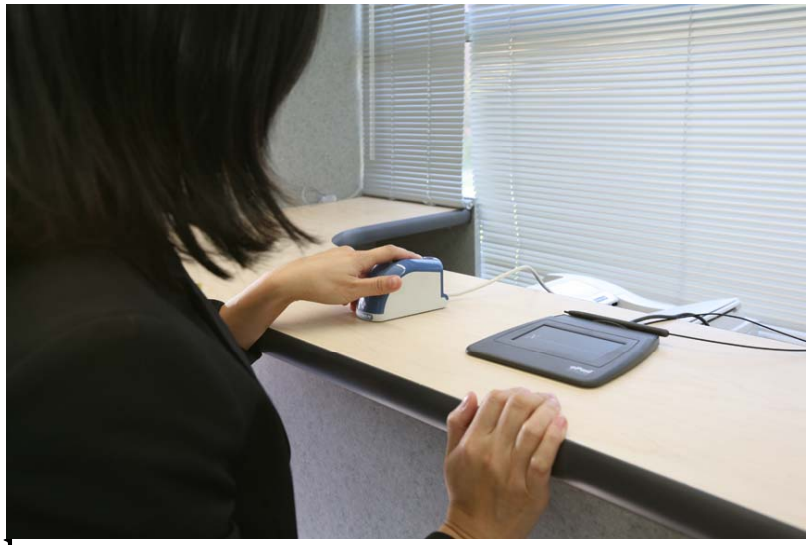
Graduate Management Admission Test® (GMAT®)

- Used in admissions' decisions by 1900 schools in over 70 countries
  - From Harvard and London Business School, HEC-Paris, to Indian School of Business, Chinese University of Hong Kong
- Administered in Pearson VUE test centers over 260,000 times in 2008 in 110 countries worldwide
  - From US, across Europe to Brazil, India, Kenya, Camp Victory Iraq

GMAT facilitates the movement of talent around the world.

Why Biometrics?

High GMAT score provides an unsurpassed opportunity for advancement.



- GMAT fraud = fraud on schools
- Unethical applicant gets into school, honest applicant left out
- 2003, 6 individuals had taken GMAT for 185 applicants
- Test security goals:
  - Maintain the integrity of the GMAT
  - Help ensure that test taker is same person who enrolls
  - Level playing field/fairness for all test takers
- Balancing security with test takers' rights

Digital Fingerprint Collection

- 2006 began collecting digital fingerprints
- Process: First-time test taker provides fingerprint at test center. Two comparisons against this original:
  1. Upon returning from break, new fingerprint compared to original.
  2. If person re-tests, new fingerprint is compared to original fingerprint.
- If no match, manual review; may not test. Other action may be taken.

Technical Challenges with Fingerprints

- Works well if B-school applicant takes GMAT, then hires imposter. No match, no test.
- Doesn't work well if applicant never takes GMAT, but only hires imposter.
- Need 1:N matching to catch imposters – not currently workable.

Legal Challenges with Fingerprints

- **United States**: No right to privacy codified in US Constitution.
  - Laissez-faire. Fine to collect/process data at will, until a problem.
  - Problems led to reactive laws, patchwork of sector and state laws.
- **Europe**: Strong sensitivity to fingerprints; Nazis, secret police.
  - Right of privacy "fundamental human right," essential to civil society, rule of law and democracy.
  - Embedded in national constitutions, European and EU law.
  - Data collection, use and transfer out of EU highly regulated.
  - EU Data Protection Directive 95/46/EC, implemented in each country, often differently.
  - Data protection authorities (DPAs), with varying powers.
  - Laws/regulators check private industry and government.

Legal Challenges with Fingerprints

Often need DPA authorization to collect biometrics.

- EU principles relevant to biometrics:
  - Notice/Consent: Clear notice and explicit, freely given consent from user required before collecting personal data. (Exceptions exist.)
  - Proportionality:
    - Suitability -- Will biometric truly fulfill intended purpose?
    - Necessity -- Is there a less intrusive means to achieve same purpose?
    - Appropriateness -- Does collection of a biometric stand in a reasonable relationship to the intrusion it will cause?
  - Security: encryption, strong security required.
- GMAC: industry leader in privacy compliance worldwide.
- But, approval by DPAs challenging. Fingerprint rejected in rare cases.

Now: Implementing Palm Vein Technology

Enhances GMAT security:

- 1:N matching on the horizon.

Designed to meet EU requirements:

- User leaves no trace on device
- No surreptitious collection
- No image stored
- Encrypted
- Unique Fujitsu-Pearson VUE algorithms:
  - Non-reversible,
  - Not interoperable with other palm vein systems.

In compliance in 99 countries, 10 of which are in Europe.

For GMAC, palm vein offers better balance between test takers' rights and test security needs.

Tips on Biometrics in Continental Europe

France, "CNIL" (Commission nationale de l'informatique et des libertés)

- CNIL's decisions followed by other EU countries
- Independent authority with stronger powers than other authorities
- Proportionality a key concern
- Interest being served is important – private/commercial or public?
- Strong security, encryption is critical
- Wary of central databases; may accept biometric card in user's control
- Only store as long as necessary; will need to justify
- Approved finger vein pattern biometric system:
  - A "traceless" biometric process, compared to DNA and fingerprints
  - No surreptitious collection possible

See also, Belgium, Privacy Commission, advisory opinion on "the processing of biometric data for the authentication of persons," 9 April 2008.

Biometrics in Private Industry

Fraud Prevention in the GMAT® Exam

Sources:

- American Bar Association, *International Guide to Privacy*, Jody Westby, ed. (2004).
- BNA, Inc., Privacy & Security Law Report, *EU Data Protection, Proportionality Principle,* Vol. 7, No. 44, 11/10/2008.
- CNIL 2007 Annual Activity Report.
- National Conference of State Legislatures.

Katherine Harman-Stokes, JD, CIPP
Associate General Counsel, Assistant Corporate Secretary
Graduate Management Admission Council® (GMAC®)
1600 Tysons Blvd., Suite 1400
McLean VA 22102
703-245-4286, kstokes@gmac.com

BIOMETRICS
TASK FORCE

BIOMETRICS
TASK FORCE

Briefing to the Government Panel
National Defense Industrial Association
January 27, 2009

Mr. Bill Vickers, Special Assistant to the Director, BTF

Terrorist Intent….

…bring the battle here

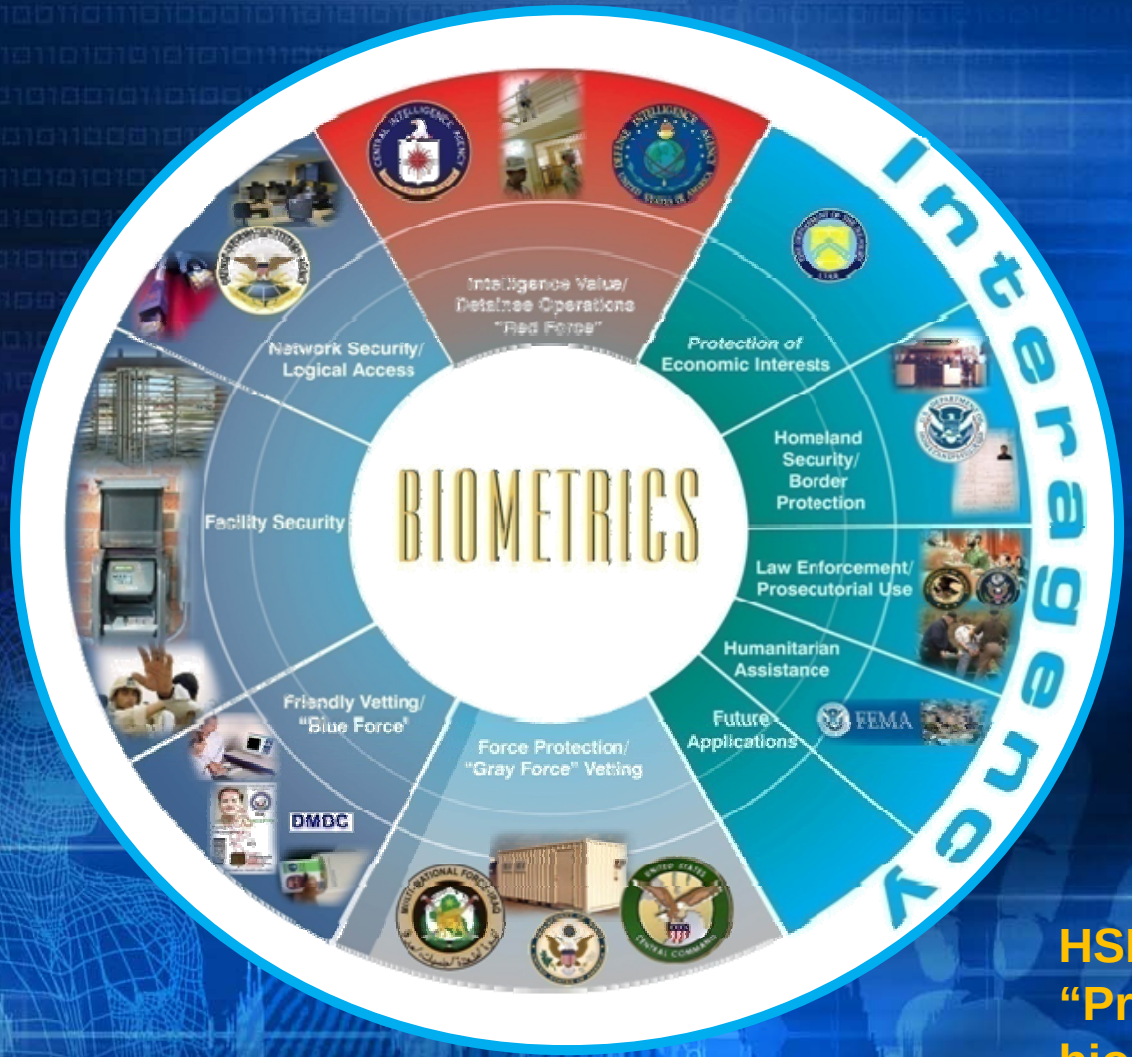
Biometrics: An Invaluable DoD Capability

- Every day, DoD collects and searches biometrics from adversaries across the globe.
- Every day, we use the data to find, track, capture, and neutralize threats against the United States.
- Every day, biometrics are used across the full spectrum of military operations, including installation access, identity screening, and intelligence, to protect U.S. interests and assets.

Our Goal: *Anyone, Anywhere, Any Time*

BIOMETRICS TASK FORCE

Across Government Workspace

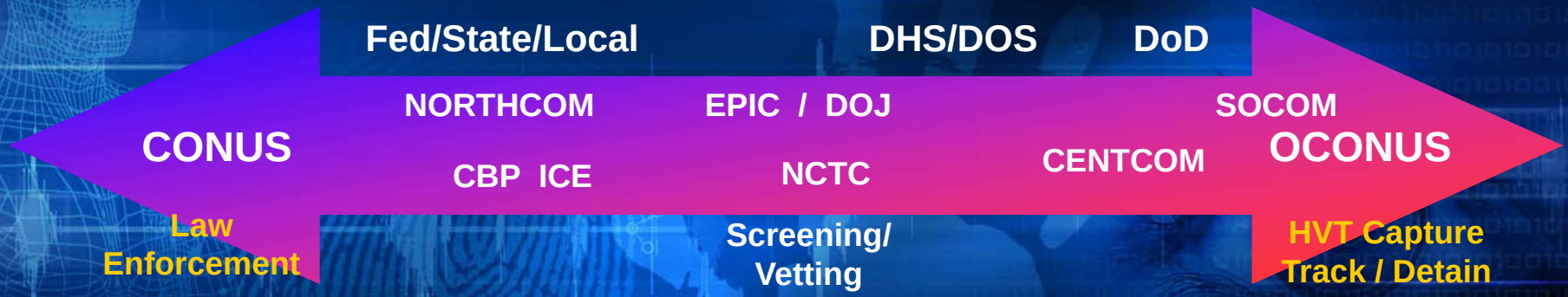


- POLICY
- PRIVACY
- LEGAL
- STANDARDS
- TECHNOLOGY

HSPD-24
"Provide for the exchange of biometric and contextual data…"

DoD's Biometric Tenets

- Our biometric intelligence and data are only valuable when the United States and our allies *use* it.
- We must continue to extend our reach to the encounter – wherever that edge may be.
- To deny enemy anonymity, we must make our biometric intelligence pervasive, authoritative, and actionable in every theater of operations.

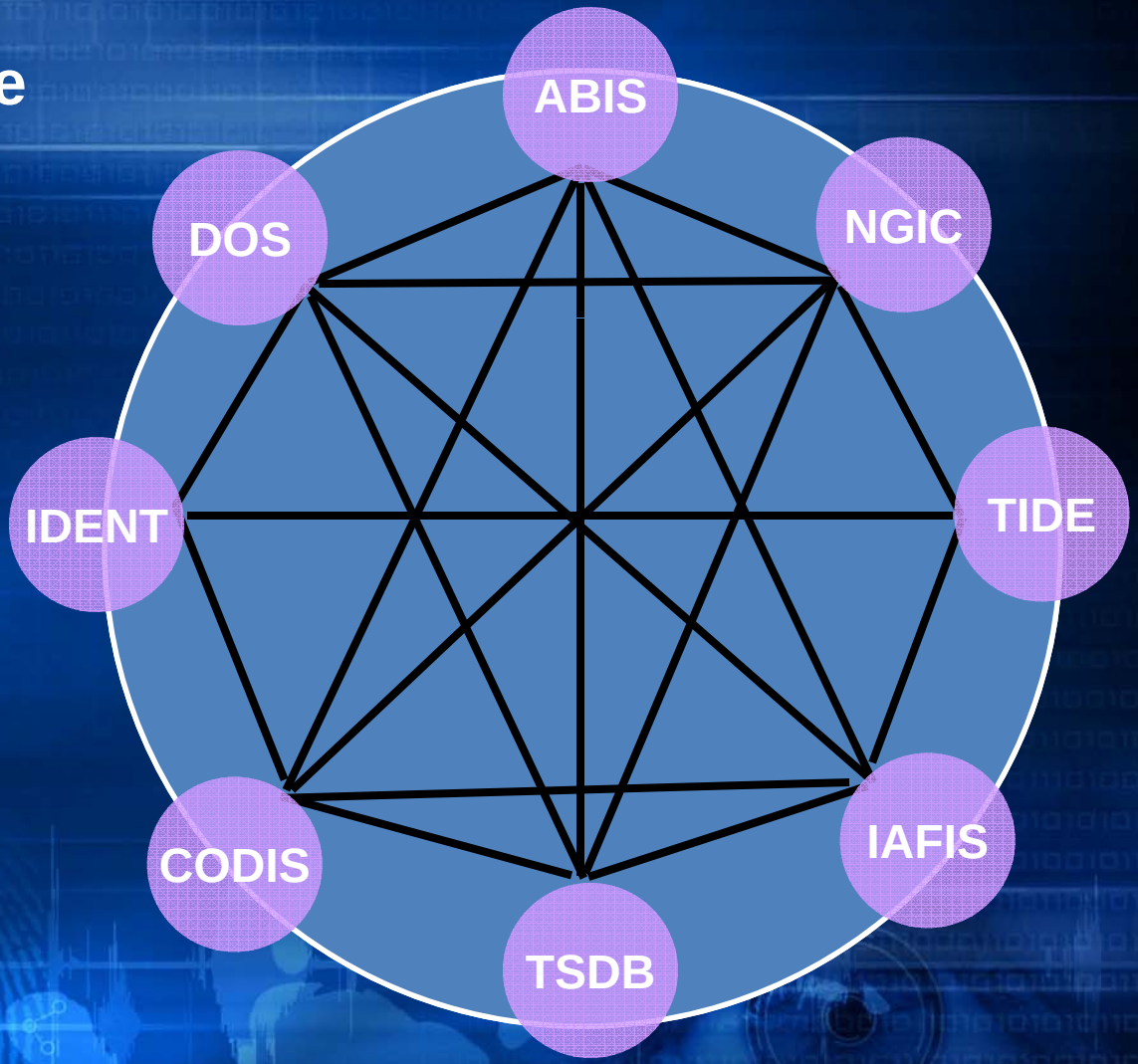


Defense in Depth

"This is the age of every Soldier as a sensor" MG John Custer

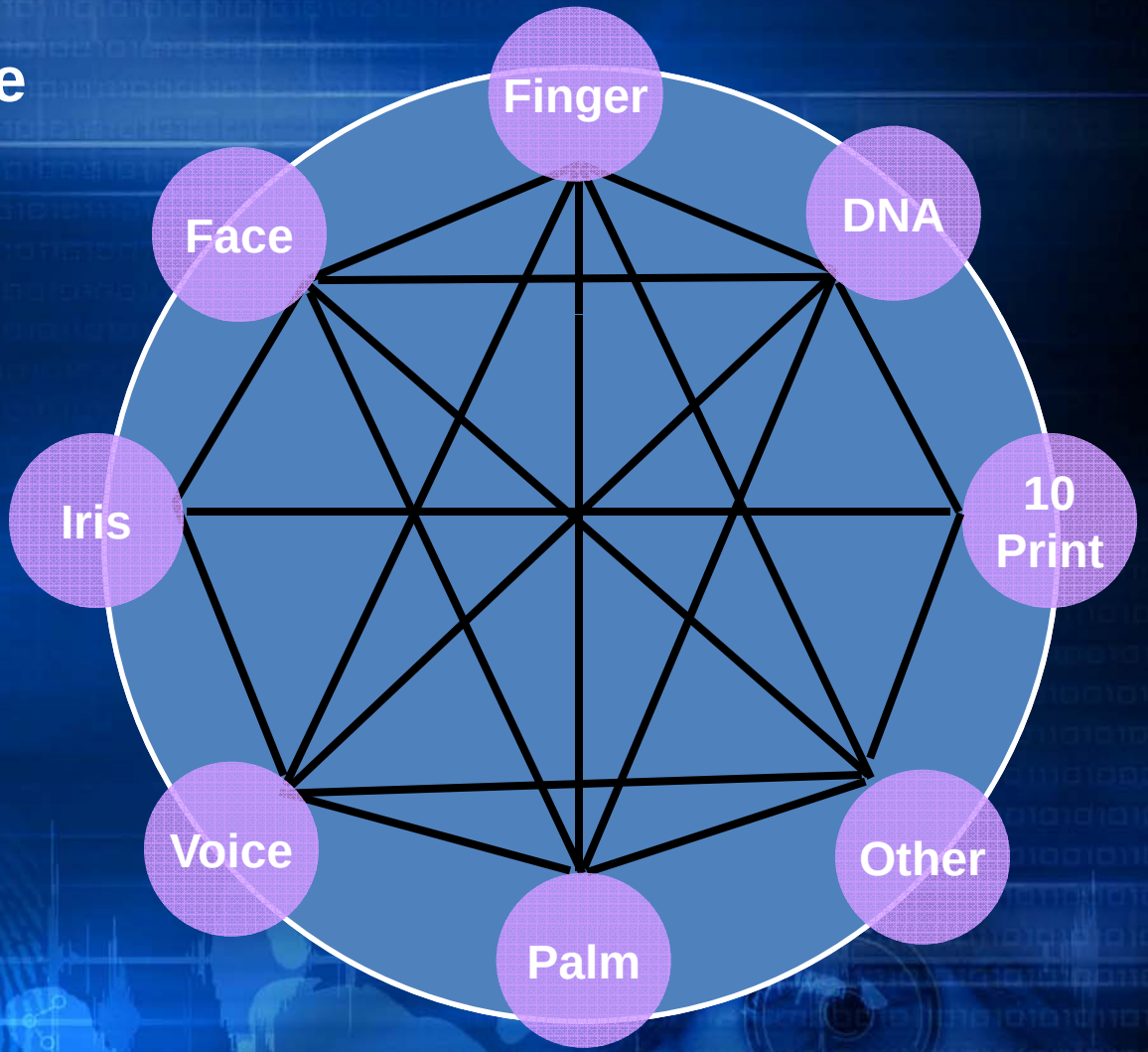
Leverage Federation

Our goal is to get on the upslope of Metcalfe's law for both systems and biometric modalities.



Leverage All Modalities

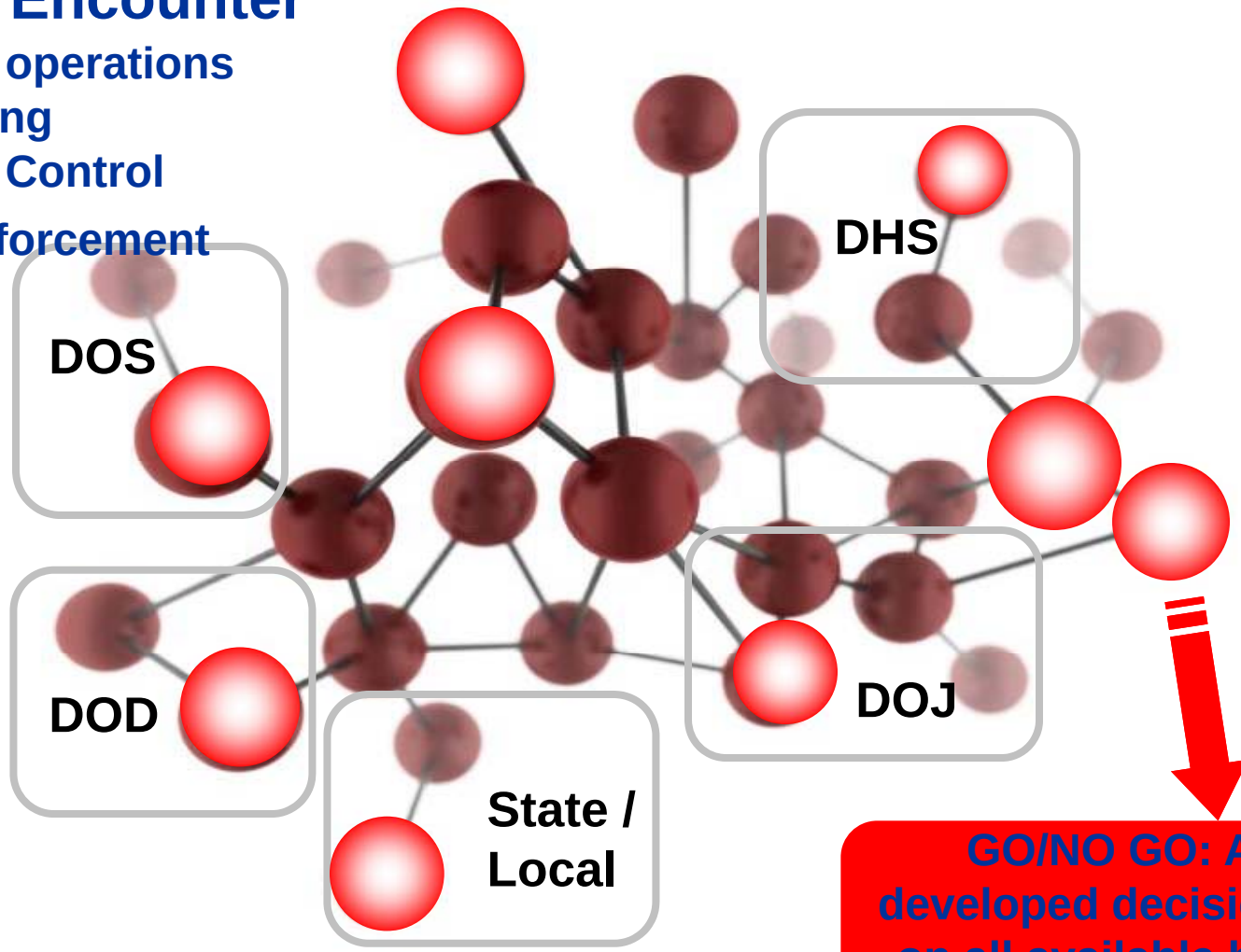
Our goal is to get on the upslope of Metcalfe's law for both systems and biometric modalities.



The Outcome:

Point of Encounter

- Military operations
- Screening
- Access Control
- Law Enforcement



GO/NO GO: A fully developed decision based on all available biometric datasets

Our Challenges

- Interoperability and standards
- Better, faster, stronger?
- The will to impact outcomes
  - Organization
  - Technology
  - Policy
- Information Sharing

Working with Industry

Industry Partners: IBIA IAI NDIA APBI

- Articulate our current and future requirements to industry; continue to engage with industry to solve our challenges.
- Invest in appropriate biometric S&T and R&D for the way ahead.

BIOMETRICS TASK FORCE

How To Reach Us

- Visit our website:
  www.biometrics.dod.mil
- E-mail us:
  hd@biometrics.dod.mil
  or
  director@biometrics.dod.mil
- Call us:
  DC - (703) 607-5000
  WV - (304) 326-3004

HSPD-24
and the Registry of Standards

Brad Wing
Biometrics Standards Coordinator

Image Group
Information Access Division
Information Technology Laboratory
National Institute of Standards and Technology

January, 2009

Recognition of the Importance of Standards

- 18) The Director of the Office of Science and Technology Policy, through the National Science and Technology Council (NSTC), shall coordinate executive branch biometric science and technology policy, including biometric standards and necessary research, development, and conformance testing programs. Recommended executive branch biometric standards are contained in the *Registry of United States Government Recommended Biometric Standards* and shall be updated via the NSTC Subcommittee on Biometrics and Identity Management.








Registry of USG Recommended Biometric Standards

http://www.biometrics.gov/Standards

Standards & Conformity Assessment Working Group (SCA WG) of the NSTC Subcommittee on Biometrics and Identity Management

Chair, Michael D. Hogan
National Institute of Standards and Technology

Your Success Depends on Knowing

- What biometric standards have been adopted for USG-wide use?
- What biometric standards will be adopted for USG-wide use?
- What kinds of USG biometric testing are required?
- What kinds of USG biometric testing will be required?

Types of Standards in the Registry

- biometric data collection, storage, and exchange standards
- biometric transmission profiles
- biometric identity credentialing profiles
- biometric technical interface standards
- biometric conformance testing methodology standards
- biometric performance testing methodology standards

The *Registry* Evolves

- As new standards, and revisions to existing standards, are approved by the standards developers, they will be evaluated for USG-wide use and may be added to the Registry.
- Two biometric modalities are clear priorities for addition to the Registry:
  - Voice
  - DNA
- Addition of ANSI/NIST-ITL 2-2008

Standards and Conformity Assessment

- ***Standards***, often, specify requirements.
- ***Conformity Assessment (CA)*** determines whether a product, service or system has fulfilled all of those requirements.

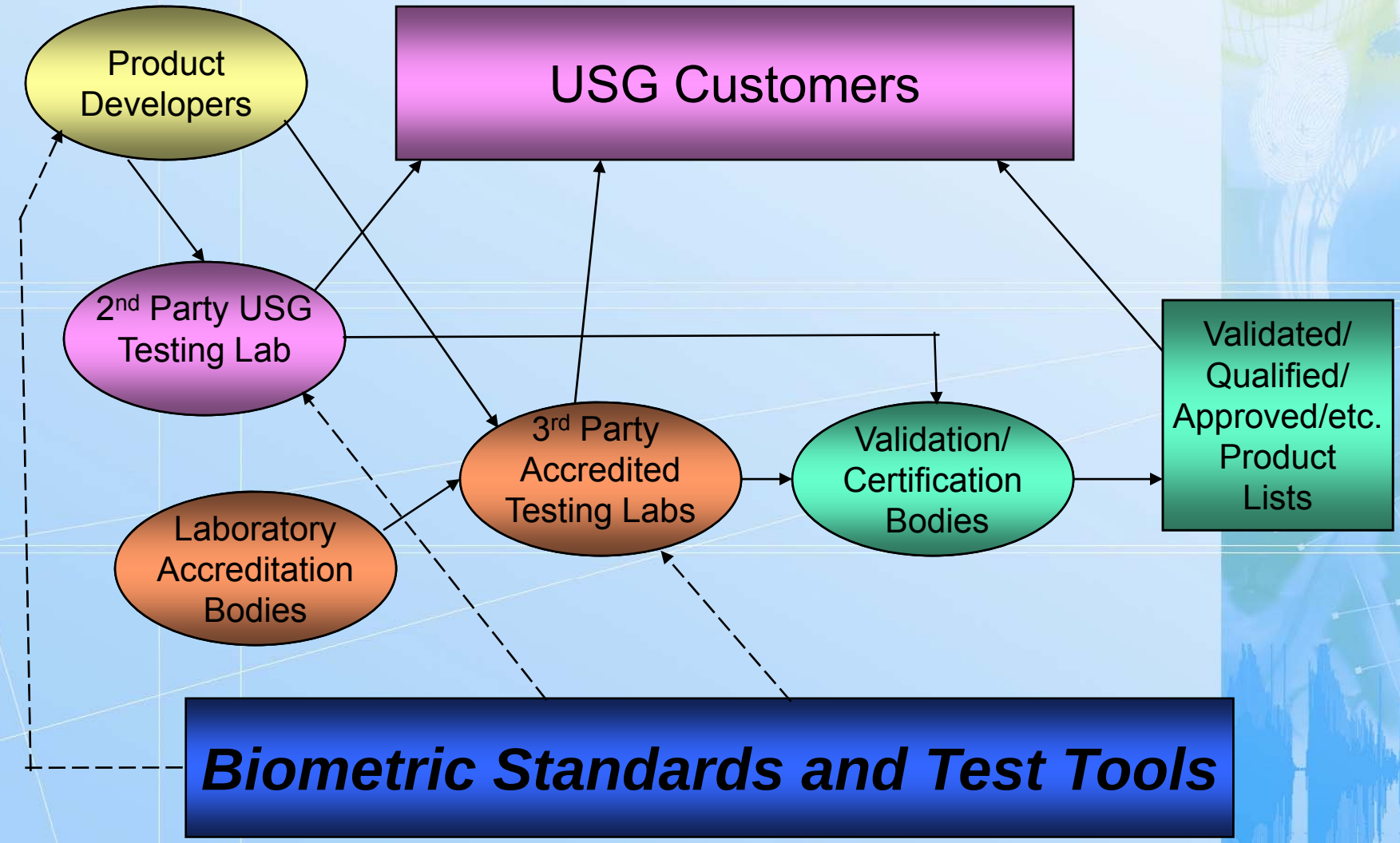
Conformity Assessment - Testing

- ***Conformance testing*** - process of checking, via test assertions, whether an implementation faithfully implements the standard or profile.
- ***Performance testing*** - measures the performance characteristics of an implementation such as system error rates, throughput, or responsiveness, under various conditions.

Conformity Assessment

- Focus:
  - development of test tools for the recommended standards;
  - 2nd party testing;
  - accreditation of 3rd party testing laboratories;
  - certification of test results.
- Terms:
  - *first party* – seller or manufacturer;
  - *second party* – purchaser or user;
  - *third party* – an independent entity that has no interest in transactions between the 1st and 2nd parties.

Robust Standards & CA Infrastructure



Conformance Test Tools for Biometric Standards

- 2005 – DoD and NIST release two cross tested test tools for BioAPI (INCITS 358-2002).
  - http://www.itl.nist.gov/div893/biometrics/BioAPI_CTS/index.htm
  - http://www.biometrics.dod.mil/CurrentInitiatives/Standards/TestingToolsets.aspx
- 2006 – NIST establishes a Minutiae Exchange Interoperability Test for INCITS 378-2004.
  - http://fingerprint.nist.gov/minex/
- August 2008 - NIST releases a conformance testing architecture and test tool for CBEFF Patron Format A (specified in INCITS 398-2008).
  - http://www.itl.nist.gov/div893/biometrics/CBEFF_PFA_CTS/index.htm

Tests Underway

- IREX08
- Multi-Biometrics Test and Evaluation
- Multiple Biometrics Grand Challenge

NIST Iris Exchange (IREX08) Test

- IREX objectives
  - Support development of interoperable iris images
    - Immediately ISO/IEC 19794-6:20XX
    - Secondarily ANSI/NIST ITL 1+2:20YY Type 17
  - Establish iris images as the primary interchange format (not templates)
  - Push developers into implementing ISO standard implementations
    - Test conformance
    - Test performance
    - Test interoperability
  - Establish compact image formats
    - Storage on smart cards (e.g. PIV)
    - Bandwidth limited networks (e.g. ship-to-shore, mobile)
  - Evaluate state-of-the-art iris recognition performance
- IREX contact point
  - http://iris.nist.gov/irex patrick.grother@nist.gov

Multi-Biometrics Test and Evaluation (MBTE)

- MBTE objectives: Evaluate the potential for iris and/or facial biometrics for use in pedestrian and maritime scenarios of exit from the U.S.

- MBTE steps:
  - Evaluate quality of face and iris images captured simultaneously under a variety of scenarios
  - Evaluate cross-camera interoperability for iris images applied to various matchers
  - Evaluate human factors impact on quality of images and FTA rate
  - Determine factors indicating need for multi-modal fusion
  - Evaluate methods for fusing multi-modal information in the specified operational scenarios

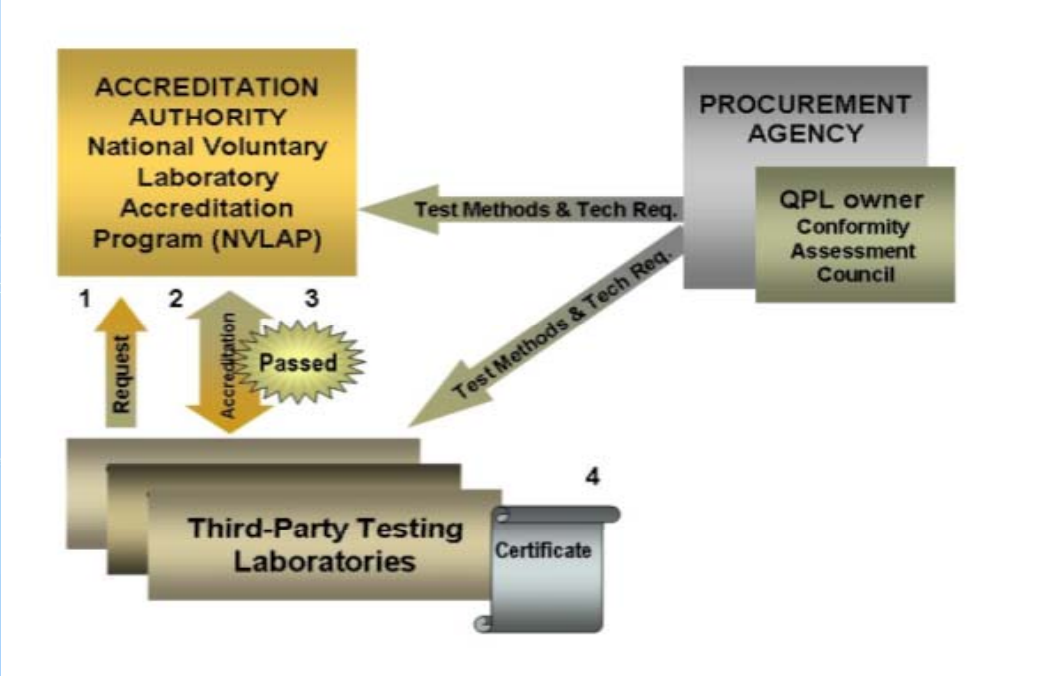
- MBTE contact points
- william.graves@dhs.gov
- patrick.grother@nist.gov

Multi-Biometric Evaluation (MBE) 2009

- Follow-up to the Multiple-Biometrics Grand Challenge 2008
- Tests to be performed by NIST using code provided by developers
  - Run against larger, sequestered data sets
  - Summer 2009 Staggered start of three tracks
    - Portal and Video
      - Executable
      - Based on FRVT 2006, ICE 2006, and MBGC
    - Still face track
      - Operational data
      - Submission of SDKs will be an option
- MBE Point of contact:
  - jonathan.phillips@nist.gov

Certified 3rd Party Product Testing Example

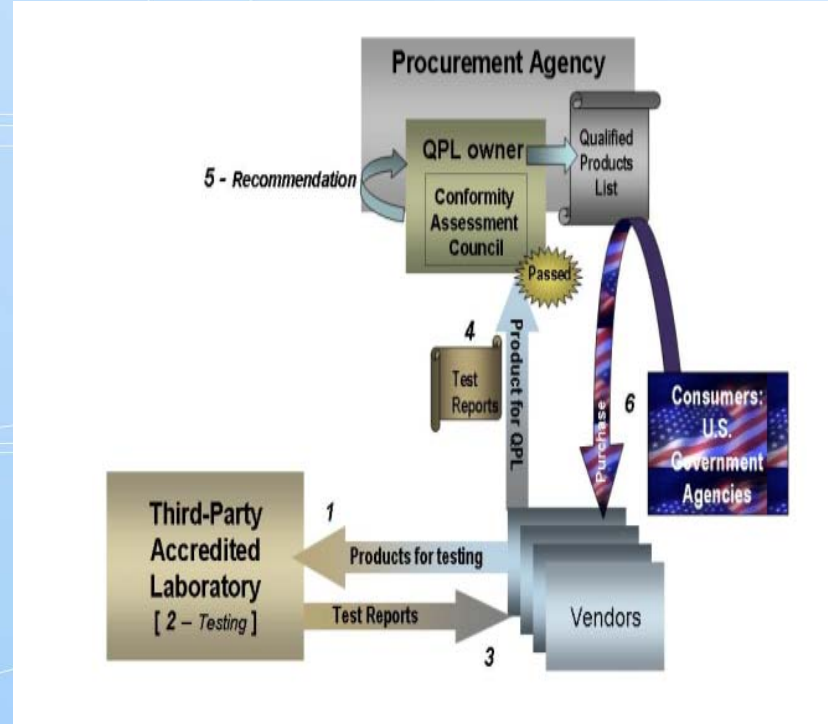
- **NIST HANDBOOK 150-25 2008 Edition**
  - National Voluntary Laboratory Accreditation Program
  - http://ts.nist.gov/Standards/Accreditation/upload/NIST-Handbook-150-25_public_draft_v1_09-18-2008.pdf



3rd Party Alternative Approaches

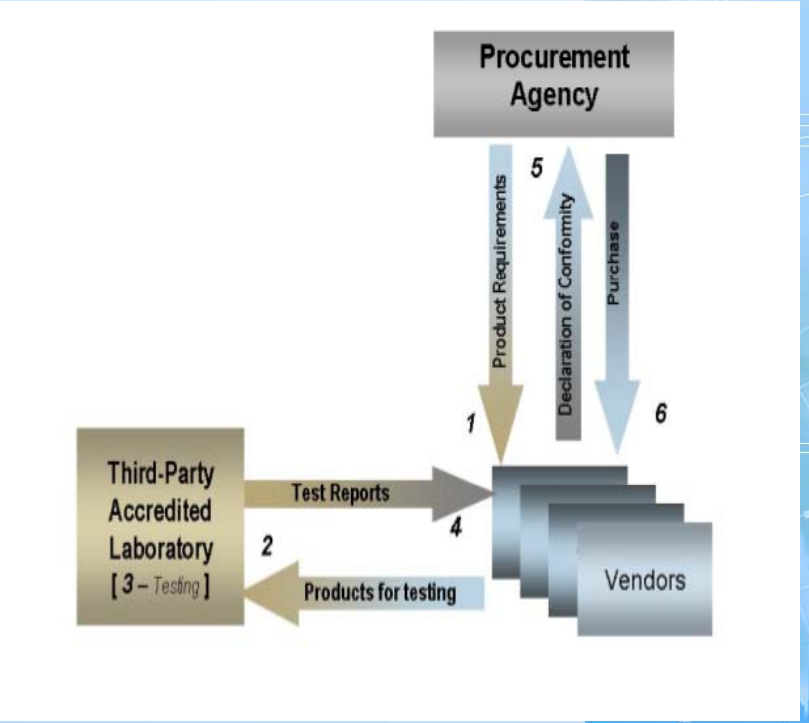
Maintained Qualified Product LIST (QPL)

►



No QPL: based on Supplier's Declaration of Conformity

►



Qualified Product Lists (QPLs) of Biometric Products

► FBI's Approved Product List of Fingerprint Scanners and Card Readers

First party testing of equipment with third party (FBI approved lab) analysis of output

General info, Appendix F in EBTS: http://www.fbibiospecs.org/fbibiometric/ebts.html

Products on QPL: http://www.fbibiospecs.org/fbibiometric/iafis.html

► TSA QPL for Biometric Airport Access Control Systems

Third party testing (TSA approved lab - transitioning to NVLAP certified labs)

General info: http://www.tsa.gov/assets/pdf/biometrics_guidance.pdf

Products on QPL: http://www.biometricgroup.com/QPL/

► Approved Product List for FIPS 201(PIV)

First, second (US Gov't -- NIST) or third party (NVLAP certified lab) testing (different procedures for various products):

General info: http://fips201ep.cio.gov/obtainlogin.php

Products on QPL: http://fips201ep.cio.gov/apl.php

Present Situation

- Groundbreaking USG-wide standards selection process is now in place.
- Augmenting the existing USG Conformity Assessment capabilities in support of the recommended standards is now underway.
- Registry will be updated as new standards emerge or older ones become obsolete

National Institute of Standards and Technology

NIST

...working with industry to foster innovation, trade, security and jobs

Brad.Wing@NIST.gov